

CIS Ubuntu Linux 22.04 LTS STIG Benchmark

v1.0.0 - 05-08-2025

Terms of Use

Please see the below link for our current terms of use:

<https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/>

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is **NEVER** acceptable to host a CIS Benchmark in **ANY** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

<i>Terms of Use</i>	<i>1</i>
<i>Table of Contents</i>	<i>2</i>
<i>Overview</i>	<i>4</i>
Important Usage Information	4
Target Technology Details	7
Intended Audience.....	7
Consensus Guidance	8
Typographical Conventions.....	9
<i>Recommendation Definitions.....</i>	<i>10</i>
Title	10
Assessment Status.....	10
Automated	10
Manual.....	10
Profile	10
Description.....	10
Rationale Statement	10
Impact Statement.....	11
Audit Procedure.....	11
Remediation Procedure.....	11
Default Value.....	11
References	11
CIS Critical Security Controls® (CIS Controls®)	11
Additional Information.....	11
Profile Definitions	12
Acknowledgements	13
<i>Recommendations</i>	<i>14</i>
<i>Appendix: Summary Table</i>	<i>407</i>
<i>Appendix: CIS Controls v7 IG 1 Mapped Recommendations</i>	<i>416</i>
<i>Appendix: CIS Controls v7 IG 2 Mapped Recommendations</i>	<i>419</i>
<i>Appendix: CIS Controls v7 IG 3 Mapped Recommendations</i>	<i>425</i>
<i>Appendix: CIS Controls v7 Unmapped Recommendations.....</i>	<i>431</i>
<i>Appendix: CIS Controls v8 IG 1 Mapped Recommendations</i>	<i>432</i>

<i>Appendix: CIS Controls v8 IG 2 Mapped Recommendations</i>	<i>436</i>
<i>Appendix: CIS Controls v8 IG 3 Mapped Recommendations</i>	<i>442</i>
<i>Appendix: CIS Controls v8 Unmapped Recommendations.....</i>	<i>448</i>
<i>Appendix: Change History</i>	<i>449</i>

Overview

All CIS Benchmarks™ (Benchmarks) focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

In the end, the Benchmarks are designed to be a key **component** of a comprehensive cybersecurity program.

Important Usage Information

All Benchmarks are available free for non-commercial use from the [CIS Website](#). They can be used to manually assess and remediate systems and applications. In lieu of manual assessment and remediation, there are several tools available to assist with assessment:

- [CIS Configuration Assessment Tool \(CIS-CAT® Pro Assessor\)](#)
- [CIS Benchmarks™ Certified 3rd Party Tooling](#)

These tools make the hardening process much more scalable for large numbers of systems and applications.

NOTE: Some tooling focuses only on the Benchmark Recommendations that can be fully automated (skipping ones marked **Manual**). It is important that **ALL** Recommendations (**Automated** and **Manual**) be addressed since all are important for properly securing systems and are typically in scope for audits.

Key Stakeholders

Cybersecurity is a collaborative effort, and cross functional cooperation is imperative within an organization to discuss, test, and deploy Benchmarks in an effective and efficient way. The Benchmarks are developed to be best practice configuration guidelines applicable to a wide range of use cases. In some organizations, exceptions to specific Recommendations will be needed, and this team should work to prioritize the problematic Recommendations based on several factors like risk, time, cost, and labor. These exceptions should be properly categorized and documented for auditing purposes.

Apply the Correct Version of a Benchmark

Benchmarks are developed and tested for a specific set of products and versions and applying an incorrect Benchmark to a system can cause the resulting pass/fail score to be incorrect. This is due to the assessment of settings that do not apply to the target systems. To assure the correct Benchmark is being assessed:

- **Deploy the Benchmark applicable to the way settings are managed in the environment:** An example of this is the Microsoft Windows family of Benchmarks, which have separate Benchmarks for Group Policy, Intune, and Stand-alone systems based upon how system management is deployed. Applying the wrong Benchmark in this case will give invalid results.
- **Use the most recent version of a Benchmark:** This is true for all Benchmarks, but especially true for cloud technologies. Cloud technologies change frequently and using an older version of a Benchmark may have invalid methods for auditing and remediation.

Exceptions

The guidance items in the Benchmarks are called recommendations and not requirements, and exceptions to some of them are expected and acceptable. The Benchmarks strive to be a secure baseline, or starting point, for a specific technology, with known issues identified during Benchmark development are documented in the Impact section of each Recommendation. In addition, organizational, system specific requirements, or local site policy may require changes as well, or an exception to a Recommendation or group of Recommendations (e.g. A Benchmark could Recommend that a Web server not be installed on the system, but if a system's primary purpose is to function as a Webserver, there should be a documented exception to this Recommendation for that specific server).

In the end, exceptions to some Benchmark Recommendations are common and acceptable, and should be handled as follows:

- The reasons for the exception should be reviewed cross-functionally and be well documented for audit purposes.
- A plan should be developed for mitigating, or eliminating, the exception in the future, if applicable.
- If the organization decides to accept the risk of this exception (not work toward mitigation or elimination), this should be documented for audit purposes.

It is the responsibility of the organization to determine their overall security policy, and which settings are applicable to their unique needs based on the overall risk profile for the organization.

Remediation

CIS has developed [Build Kits](#) for many technologies to assist in the automation of hardening systems. Build Kits are designed to correspond to Benchmark's "Remediation" section, which provides the manual remediation steps necessary to make that Recommendation compliant to the Benchmark.

When remediating systems (changing configuration settings on deployed systems as per the Benchmark's Recommendations), please approach this with caution and test thoroughly.

The following is a reasonable remediation approach to follow:

- CIS Build Kits, or internally developed remediation methods should never be applied to production systems without proper testing.
- Proper testing consists of the following:
 - Understand the configuration (including installed applications) of the targeted systems. Various parts of the organization may need different configurations (e.g., software developers vs standard office workers).
 - Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.
 - Test the configuration changes with representative lab system(s). If issues arise during testing, they can be resolved prior to deploying to any production systems.
 - When testing is complete, initially deploy to a small sub-set of production systems and monitor closely for issues. If there are issues, they can be resolved prior to deploying more broadly.
 - When the initial deployment above is completed successfully, iteratively deploy to additional systems and monitor closely for issues. Repeat this process until the full deployment is complete.

Summary

Using the Benchmarks Certified tools, working as a team with key stakeholders, being selective with exceptions, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

NOTE: As previously stated, the PDF versions of the CIS Benchmarks™ are available for free, non-commercial use on the [CIS Website](#). All other formats of the CIS Benchmarks™ (MS Word, Excel, and [Build Kits](#)) are available for CIS [SecureSuite®](#) members.

CIS-CAT® Pro is also available to CIS [SecureSuite®](#) members.

Target Technology Details

Canonical Ubuntu 22.04 LTS Secure Technical Implementation Guide (STIG) Version: 2
Release: 4 Benchmark Date: 02 Apr 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Canonical Ubuntu 22.04 LTS and are looking to comply with the STIG guidance

Consensus Guidance

This CIS Benchmark™ was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit <https://workbench.cisecurity.org/>.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
<code>Stylized Monospace font</code>	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
<code>Monospace font</code>	Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented.
<code><Monospace font in brackets></code>	Text set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication.
Bold font	Additional information or caveats things like Notes , Warnings , or Cautions (usually just the word itself and the rest of the text normal).

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) "4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

Items in this profile exhibit one or more of the following characteristics:

- are considered to be high severity
- are intended for environments or use cases where following STIG based security guidance is paramount.
- acts as defense in depth measure.
- may negatively inhibit the utility or performance of the technology.

This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

Items in this profile exhibit one or more of the following characteristics:

- are considered to be medium severity
- are intended for environments or use cases where following STIG based security guidance is paramount.
- acts as defense in depth measure.
- may negatively inhibit the utility or performance of the technology.

This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

Items in this profile exhibit one or more of the following characteristics:

- are considered to be low severity
- are intended for environments or use cases where following STIG based security guidance is paramount.
- acts as defense in depth measure.
- may negatively inhibit the utility or performance of the technology.

This profile is intended for servers and workstations.

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Canonical Ubuntu 22.04 LTS

Contributor

Randie Bejar
Eric Pinnell
Gokhan Lus
Michael Wood

Recommendations

1 STIG RULES

Canonical Ubuntu 22.04 LTS

Secure Technical Implementation Guide (STIG)

Version: 2 Release: 4 Benchmark

Date: 02 Apr 2025

CLASSIFICATION unclassified

Note: References to CIS Recommendations are from the CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0

1.1 UBTU-22-211015 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

The operating system must disable the x86 Ctrl-Alt-Delete key sequence.

```
GROUP ID: V-260469
RULE ID: SV-260469r991589
```

Rationale:

A locally logged-on user who presses Ctrl-Alt-Delete, when at the console, can reboot the system. If accidentally pressed, as could happen in the case of a mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot.

Audit:

Verify the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed by using the following command:

```
$ systemctl status ctrl-alt-del.target

ctrl-alt-del.target
  Loaded: masked (Reason: Unit ctrl-alt-del.target is masked.)
  Active: inactive (dead)
```

If the "ctrl-alt-del.target" is not masked, this is a finding.

Remediation:

Configure the operating system to disable the Ctrl-Alt-Delete sequence for the command line by using the following commands:

```
$ sudo systemctl disable ctrl-alt-del.target
$ sudo systemctl mask ctrl-alt-del.target
```

Reload the daemon to take effect:







```
$ sudo systemctl daemon-reload
```


Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.2 UBTU-22-212010 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

The operating system, when booted, must require authentication upon booting into single-user and maintenance modes.

GROUP ID: V-260470 RULE ID: SV-260470r958472

Rationale:

To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DOD-approved PKIs, all DOD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access.

Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Audit:

Verify the operating system requires a password for authentication upon booting into single-user and maintenance modes by using the following command:

```
$ sudo grep -i password /boot/grub/grub.cfg

password_pbkdf2 root
grub.pbkdf2.sha512.10000.03255F190F0E2F7B4F0D1C3216012309162F022A7A636771
```

If the root password entry does not begin with "password_pbkdf2", this is a finding.

Remediation:

Configure the operating system to require a password for authentication upon booting into single-user and maintenance modes.

Generate an encrypted (grub) password for root by using the following command:

```
$ grub-mkpasswd-pbkdf2

Enter Password:
Reenter Password:
PBKDF2 hash of your password is
grub.pbkdf2.sha512.10000.03255F190F0E2F7B4F0D1C3216012309162F022A7A636771
```

Using the hash from the output, modify the "/etc/grub.d/40_custom" file by using the following command to add a boot password:

```
$ sudo sed -i '$i set superusers=\"root\"\\npasswd_pbkdf2 root <hash>'
/etc/grub.d/40_custom
```

where is the hash generated by grub-mkpasswd-pbkdf2 command.

Generate an updated "grub.conf" file with the new password by using the following command:

```
$ sudo update-grub
```

References:






1. CIS Recommendation "Ensure bootloader password is set"

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53 :: AC-3
- NIST SP 800-53 Revision 4 :: AC-3
- NIST SP 800-53 Revision 5 :: AC-3
- NIST SP 800-53A :: AC-3.1

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 <u>Use Unique Passwords</u> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

1.3 UBTU-22-212015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must initiate session audits at system startup.

```
GROUP ID: V-260471
RULE ID: SV-260471r1069117
```

Rationale:

If auditing is enabled late in the startup process, the actions of some startup processes may not be audited. Some audit systems also maintain state information only available if auditing is enabled before a given process is created.

Audit:

Verify that the operating system enables auditing at system startup in grub by using the following command:

```
$ grep "^\\s*linux" /boot/grub/grub.cfg

linux    /vmlinuz-5.15.0-89-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro
audit=1
linux    /vmlinuz-5.15.0-89-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro
audit=1
linux    /vmlinuz-5.15.0-89-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro
single nomodeset dis_ucode_ldr audit=1
linux    /vmlinuz-5.15.0-83-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro
audit=1
linux    /vmlinuz-5.15.0-83-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro
single nomodeset dis_ucode_ldr audit=1
```

If any linux lines do not contain "audit=1", this is a finding.

Note: Output may vary by system.

Remediation:

Configure the operating system to produce audit records at system startup.

Edit the "/etc/default/grub" file and add "audit=1" to the "GRUB_CMDLINE_LINUX" option and to the "GRUB_CMDLINE_LINUX_DEFAULT" option.

```
GRUB_CMDLINE_LINUX_DEFAULT="audit=1"
GRUB_CMDLINE_LINUX="audit=1"
```

To update the grub config file, run:

```
$ sudo update-grub
```

References:







1. CIS Recommendation "Ensure auditing for processes that start prior to auditd is enabled"

Additional Information:

CCI-001464 Initiates session audits automatically at system start-up.

- NIST SP 800-53 :: AU-14 (1)
- NIST SP 800-53 Revision 4 :: AU-14 (1)
- NIST SP 800-53 Revision 5 :: AU-14 (1)
- NIST SP 800-53A :: AU-14 (1).1

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.2 <u>Establish an Access Revoking Process</u> Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

1.4 UBTU-22-213010 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must restrict access to the kernel message buffer.

```
GROUP ID: V-260472
RULE ID: SV-260472r958524
```

Rationale:

Restricting access to the kernel message buffer limits access only to root. This prevents attackers from gaining additional system information as a nonprivileged user.

Audit:

Verify the operating system is configured to restrict access to the kernel message buffer by using the following command:

```
$ sysctl kernel.dmesg_restrict

kernel.dmesg_restrict = 1
```

If "kernel.dmesg_restrict" is not set to "1" or is missing, this is a finding.

Verify that there are no configurations that enable the kernel dmesg function:

```
$ sudo grep -ir kernel.dmesg_restrict /run/sysctl.d/* /etc/sysctl.d/*
/usr/local/lib/sysctl.d/* /usr/lib/sysctl.d/* /lib/sysctl.d/*
/etc/sysctl.conf 2> /dev/null

/etc/sysctl.d/10-kernel-hardening.conf:kernel.dmesg_restrict = 1
```

If "kernel.dmesg_restrict" is not set to "1", is commented out, is missing, or conflicting results are returned, this is a finding.

Remediation:

Configure the operating system to restrict access to the kernel message buffer.
Add or modify the following line in the "/etc/sysctl.conf" file:

```
kernel.dmesg_restrict = 1
```

Remove any configurations that conflict with the above from the following locations:

/run/sysctl.d/

/etc/sysctl.d/

/usr/local/lib/sysctl.d/

/usr/lib/sysctl.d/

/lib/sysctl.d/

/etc/sysctl.conf

Reload settings from all system configuration files by using the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-001090 Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53 :: SC-4
- NIST SP 800-53 Revision 4 :: SC-4
- NIST SP 800-53 Revision 5 :: SC-4
- NIST SP 800-53A :: SC-4.1

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

1.5 UBTU-22-213015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must disable kernel core dumps so that it can fail to a secure state if system initialization fails, shutdown fails or aborts fail.

```
GROUP ID: V-260473
RULE ID: SV-260473r1044782
```

Rationale:

Kernel core dumps may contain the full contents of system memory at the time of the crash. Kernel core dumps may consume a considerable amount of disk space and may result in denial of service by exhausting the available space on the target file system partition.

Audit:

Verify that kernel core dumps are disabled unless needed by using the following command:

```
$ systemctl status kdump-tools.service

kdump-tools.service
  Loaded: masked (Reason: Unit kdump-tools.service is masked.)
  Active: inactive (dead)
```

If "kdump-tools.service" is not masked and inactive, ask the system administrator (SA) if the use of the service is required and documented with the information system security officer (ISSO).

If the service is active and is not documented, this is a finding.

Remediation:

If kernel core dumps are not required, disable and mask "kdump-tools.service" by using the following command:

```
$ sudo systemctl mask kdump-tools --now
```





If kernel core dumps are required, document the need with the ISSO.

Additional Information:

CCI-001190 Fail to an organization-defined known-system state for the following failures on the indicated components while preserving organization-defined system state information in failure.

- NIST SP 800-53 :: SC-24
- NIST SP 800-53 Revision 4 :: SC-24
- NIST SP 800-53 Revision 5 :: SC-24
- NIST SP 800-53A :: SC-24.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

1.6 UBTU-22-213020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must implement address space layout randomization to protect its memory from unauthorized code execution.

```
GROUP ID: V-260474
RULE ID: SV-260474r958928
```

Rationale:

Some adversaries launch attacks with the intent of executing code in nonexecutable regions of memory or in prohibited memory locations. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.

Examples of attacks are buffer overflow attacks.

Audit:

Verify the operating system implements address space layout randomization (ASLR) by using the following command:

```
$ sysctl kernel.randomize_va_space
kernel.randomize_va_space = 2
```

If no output is returned, verify the kernel parameter "randomize_va_space" is set to "2" by using the following command:

```
$ cat /proc/sys/kernel/randomize_va_space
2
```

If "kernel.randomize_va_space" is not set to "2", this is a finding.

Verify that a saved value of the "kernel.randomize_va_space" variable is not defined:

```
$ sudo grep -ER "^kernel.randomize_va_space=[^2]" /etc/sysctl.conf
/etc/sysctl.d
```

If this returns a result, this is a finding.

Remediation:

Remove the "kernel.randomize_va_space" entry found in the "/etc/sysctl.conf" file or any file located in the "/etc/sysctl.d/" directory.

Reload the system configuration files for the changes to take effect by using the following command:

```
$ sudo sysctl --system
```

References:

1. CIS Recommendation "Ensure address space layout randomization is enabled"

Additional Information:

CCI-002824 Implement organization-defined controls to protect its memory from unauthorized code execution.

- NIST SP 800-53 Revision 4 :: SI-16
- NIST SP 800-53 Revision 5 :: SI-16

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

1.7 UBTU-22-213025 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must implement nonexecutable data to protect its memory from unauthorized code execution.

```
GROUP ID: V-260475
RULE ID: SV-260475r958928
```

Rationale:

Some adversaries launch attacks with the intent of executing code in nonexecutable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.

Examples of attacks are buffer overflow attacks.

Audit:

Verify the NX (no-execution) bit flag is set on the system by using the following command:

```
$ sudo dmesg | grep -i "execute disable"

[    0.000000] NX (Execute Disable) protection: active
```

If "dmesg" does not show "NX (Execute Disable) protection: active", check the hardware capabilities of the installed CPU by using the following command:

```
$ grep flags /proc/cpuinfo | grep -o nx | sort -u

nx
```

If no output is returned, this is a finding.

Remediation:

Configure the operating system to enable NX.





If the installed CPU is hardware capable of NX protection, check if the system's BIOS/UEFI setup configuration permits toggling the "NX bit" or "no execution bit", and set it to "enabled".

Additional Information:

CCI-002824 Implement organization-defined controls to protect its memory from unauthorized code execution.

- NIST SP 800-53 Revision 4 :: SI-16
- NIST SP 800-53 Revision 5 :: SI-16

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.			
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.			

1.8 UBTU-22-214010 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must be configured so that the Advance Package Tool (APT) prevents the installation of patches, service packs, device drivers, or operating system components without verification they have been digitally signed using a certificate that is recognized and approved by the organization.

```
GROUP ID: V-260476
RULE ID: SV-260476r1015003
```

Rationale:

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This ensures the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DOD certificates for this purpose; however, the certificate used to verify the software must be from an approved certificate authority (CA).

Audit:

Verify that APT is configured to prevent the installation of patches, service packs, device drivers, or Ubuntu operating system components without verification they have been digitally signed using a certificate that is recognized and approved by the organization by using the following command:

```
$ grep -i allowunauthenticated /etc/apt/apt.conf.d/*
/etc/apt/apt.conf.d/01-vendor-ubuntu:APT::Get::AllowUnauthenticated "false";
```

If "APT::Get::AllowUnauthenticated" is not set to "false", is commented out, or is missing, this is a finding.

Remediation:

Configure APT to prevent the installation of patches, service packs, device drivers, or Ubuntu operating system components without verification they have been digitally signed using a certificate that is recognized and approved by the organization. Add or modify the following line in any file under the "/etc/apt/apt.conf.d/" directory:

```
APT::Get::AllowUnauthenticated "false";
```

Additional Information:







CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5 :: CM-14

CCI-001749 The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 4 :: CM-5 (3)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>7.3 Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<u>3.4 Deploy Automated Operating System Patch Management Tools</u> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.			

1.9 UBTU-22-214015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must be configured so that the Advance Package Tool (APT) removes all software components after updated versions have been installed.

```
GROUP ID: V-260477
RULE ID: SV-260477r1044773
```

Rationale:

Previous versions of software components that are not removed from the information system after updates have been installed may be exploited by adversaries. Some information technology products may remove older versions of software automatically from the information system.

Audit:

Verify APT is configured to remove all software components after updated versions have been installed by using the following command:

```
$ grep -i remove-unused /etc/apt/apt.conf.d/50unattended-upgrades

Unattended-Upgrade::Remove-Unused-Kernel-Packages "true";
Unattended-Upgrade::Remove-Unused-Dependencies "true";
```

If "Unattended-Upgrade::Remove-Unused-Kernel-Packages" and "Unattended-Upgrade::Remove-Unused-Dependencies" are not set to "true", are commented out, or are missing, this is a finding.

Remediation:

Configure APT to remove all software components after updated versions have been installed.

Add or modify the following lines in the "/etc/apt/apt.conf.d/50unattended-upgrades" file:

```
Unattended-Upgrade::Remove-Unused-Kernel-Packages "true";
Unattended-Upgrade::Remove-Unused-Dependencies "true";
```

Additional Information:

CCI-002617 Remove previous versions of organization-defined software components after updated versions have been installed.

- NIST SP 800-53 Revision 4 :: SI-2 (6)
- NIST SP 800-53 Revision 5 :: SI-2 (6)

1.10 UBTU-22-215010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must have the "libpam-pwquality" package installed.

```
GROUP ID: V-260478
RULE ID: SV-260478r991587
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. "pwquality" enforces complex password construction configuration and has the ability to limit brute-force attacks on the system.

Audit:

Verify the operating system has the "libpam-pwquality" package installed with the following command:

```
$ dpkg -l | grep libpam-pwquality

ii      libpam-pwquality:amd64      1.4.4-1build2      amd64      PAM module to
check password strength
```

If "libpam-pwquality" is not installed, this is a finding.

Remediation:

Install the "pam_pwquality" package by using the following command:

```
$ sudo apt-get install libpam-pwquality
```

References:

1. CIS Recommendation "Ensure libpam-pwquality is installed"

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.11 UBTU-22-215015 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must have the "chrony" package installed.

```
GROUP ID: V-260479
RULE ID: SV-260479r991589
```

Rationale:

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Organizations must consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

Audit:

Verify the "chrony" package is installed using the following command:

```
$ dpkg -l | grep chrony

ii      chrony      4.2-2ubuntu2      amd64      Versatile implementation of the
Network Time Protocol
```

If the "chrony" package is not installed, this is a finding.

Remediation:

Install the "chrony" network time protocol package using the following command:





```
$ sudo apt-get install chrony
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 <u>Standardize Time Synchronization</u> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.			
v7	6.1 <u>Utilize Three Synchronized Time Sources</u> Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.			

1.12 UBTU-22-215020 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must not have the "systemd-timesyncd" package installed.

```
GROUP ID: V-260480
RULE ID: SV-260480r991589
```

Rationale:

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Organizations must consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

Audit:

Verify that the "systemd-timesyncd" package is not installed by using the following command:

```
$ dpkg -l | grep systemd-timesyncd
```

If the "systemd-timesyncd" package is installed, this is a finding.

Remediation:

The "systemd-timesyncd" package will be uninstalled as part of the "chrony" package install. The remaining configuration files for "systemd-timesyncd" must be purged from the operating system:

```
$ sudo dpkg -P --force-all systemd-timesyncd
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 <u>Standardize Time Synchronization</u> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	6.1 <u>Utilize Three Synchronized Time Sources</u> Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

1.13 UBTU-22-215025 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must not have the "ntp" package installed.

```
GROUP ID: V-260481
RULE ID: SV-260481r991589
```

Rationale:

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Organizations must consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

Audit:

Verify that the "ntp" package is not installed by using the following command:

```
$ dpkg -l | grep ntp
```

If the "ntp" package is installed, this is a finding.

Remediation:

Uninstall the "ntp" package by using the following command:

```
$ sudo dpkg -P --force-all ntp
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 <u>Standardize Time Synchronization</u> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	6.1 <u>Utilize Three Synchronized Time Sources</u> Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

1.14 UBTU-22-215030 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

The operating system must not have the "rsh-server" package installed.

```
GROUP ID: V-260482
RULE ID: SV-260482r958478
```

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Remote Shell (RSH) is a client/server application protocol that provides an unencrypted remote access service, which does not provide for the confidentiality and integrity of user passwords or the remote session. If users were allowed to login to a system using RSH, the privileged user passwords and communications could be compromised.

Removing the "rsh-server" package decreases the risk of accidental or intentional activation of the RSH service.

Audit:

Verify the "rsh-server" package is not installed by using the following command:

```
$ dpkg -l | grep rsh-server
```

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

Remediation:

Remove the "rsh-server" package by using the following command:

```
$ sudo apt-get remove rsh-server
```

References:





1. CIS Recommendation "Ensure rsh-server is not installed"

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

1.15 UBTU-22-215035 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

The operating system must not have the "telnet" package installed.

```
GROUP ID: V-260483
RULE ID: SV-260483r987796
```

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities are often overlooked and therefore, may remain unsecure. They increase the risk to the platform by providing additional attack vectors.

Telnet is a client/server application protocol that provides an unencrypted remote access service, which does not provide for the confidentiality and integrity of user passwords or the remote session. If users were allowed to login to a system using Telnet, the privileged user passwords and communications could be compromised.

Removing the "telnetd" package decreases the risk of accidental or intentional activation of the Telnet service.

Audit:

Verify that the "telnetd" package is not installed on the operating system by using the following command:

```
$ dpkg -l | grep telnetd
```

If the "telnetd" package is installed, this is a finding.

Remediation:

Remove the "telnetd" package by using the following command:

```
$ sudo apt-get remove telnetd
```

References:





1. CIS Recommendation "Ensure telnetd is not installed"

Additional Information:

CCI-000197 For password-based authentication, transmit passwords only cryptographically-protected channels.

- NIST SP 800-53 :: IA-5 (1) (c)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (c)
- NIST SP 800-53 Revision 5 :: IA-5 (1) (c)
- NIST SP 800-53A :: IA-5 (1).1 (v)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

1.16 UBTU-22-231010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must implement cryptographic mechanisms to prevent unauthorized disclosure and modification of all information that requires protection at rest.

GROUP ID: V-260484 RULE ID: SV-260484r958552

Rationale:

Operating systems handling data requiring "data at rest" protections must employ cryptographic mechanisms to prevent unauthorized disclosure and modification of the information at rest.

Selection of a cryptographic mechanism is based on the need to protect the integrity of organizational information. The strength of the mechanism is commensurate with the security category and/or classification of the information. Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields).

Satisfies: SRG-OS-000185-GPOS-00079, SRG-OS-000404-GPOS-00183, SRG-OS-000405-GPOS-00184

Audit:

Verify the operating system prevents unauthorized disclosure or modification of all information requiring at-rest protection by using disk encryption.

Note: If there is a documented and approved reason for not having data-at-rest encryption, this requirement is not applicable.

Determine the partition layout for the system by using the following command:

```
$ sudo fdisk -l
```

...						
Device		Start		End	Sectors	Size Type
/dev/sda1		2048	2203647	2201600	1G	EFI System
/dev/sda2	2203648	6397951	4194304		2G	Linux filesystem
/dev/sda3	6397952	536868863	530470912	252.9G		Linux filesystem
...						

Verify the system partitions are all encrypted by using the following command:

```
# more /etc/crypttab
```

Every persistent disk partition present must have an entry in the file.

If any partitions other than the boot partition or pseudo file systems (such as /proc or /sys) are not listed, this is a finding.

Remediation:

To encrypt an entire partition, dedicate a partition for encryption in the partition layout.

Note: Encrypting a partition in an already-installed system is more difficult because it will need to be resized and existing partitions changed.

Additional Information:

CCI-001199 Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53 :: SC-28
- NIST SP 800-53 Revision 4 :: SC-28
- NIST SP 800-53 Revision 5 :: SC-28
- NIST SP 800-53A :: SC-28.1




CCI-002475 Implement cryptographic mechanisms to prevent unauthorized modification of organization-defined information when at rest on organization-defined system components.

- NIST SP 800-53 Revision 4 :: SC-28 (1)
- NIST SP 800-53 Revision 5 :: SC-28 (1)

CCI-002476 Implement cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined system components.

- NIST SP 800-53 Revision 4 :: SC-28 (1)
- NIST SP 800-53 Revision 5 :: SC-28 (1)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

1.17 UBTU-22-232010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must have directories that contain system commands set to a mode of "755" or less permissive.

```
GROUP ID: V-260485
RULE ID: SV-260485r991559
```

Rationale:

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

Operating systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools and the corresponding rights the user has in order to make access decisions regarding the deletion of audit tools.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Audit:

Verify the system commands directories have mode "755" or less permissive by using the following command:

```
$ find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin -perm /022 -type d -exec stat -c "%n %a" '{}' \;
```

If any directories are found to be group-writable or world-writable, this is a finding.

Remediation:

Configure the operating system commands directories to be protected from unauthorized access. Run the following command:







```
$ sudo find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin -perm /022 -type d -exec chmod -R 755 '{}' \;
```


Additional Information:

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9
- NIST SP 800-53A :: AU-9.1

CIS Controls:

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

1.18 UBTU-22-232015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must have system commands set to a mode of "755" or less permissive.

```
GROUP ID: V-260486
RULE ID: SV-260486r991560
```

Rationale:

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to the operating system with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system commands contained in the following directories have mode "755" or less permissive by using the following command:

```
$ sudo find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin -
perm /022 -type f -exec stat -c "%n %a" '{}' \;
```

If any files are found to be group-writable or world-writable, this is a finding.

Remediation:

Configure the operating system commands to be protected from unauthorized access. Run the following command:







```
$ sudo find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin -
perm /022 -type f -exec chmod 755 '{}' \;
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53 :: CM-5 (6)
- NIST SP 800-53 Revision 4 :: CM-5 (6)
- NIST SP 800-53 Revision 5 :: CM-5 (6)
- NIST SP 800-53A :: CM-5 (6).1

CIS Controls:

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

1.19 UBTU-22-232020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system library files must have mode "755" or less permissive.

```
GROUP ID: V-260487
RULE ID: SV-260487r991560
```

Rationale:

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the systemwide shared library files contained in the directories "/lib", "/lib64", and "/usr/lib" have mode "755" or less permissive by using the following command:

```
$ sudo find /lib /lib64 /usr/lib -perm /022 -type f -exec stat -c "%n %a"
'{}' \;
```

If any files are found to be group-writable or world-writable, this is a finding.

Remediation:

Configure the library files to be protected from unauthorized access. Run the following command:







```
$ sudo find /lib /lib64 /usr/lib -perm /022 -type f -exec chmod 755 '{} ' \;
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53 :: CM-5 (6)
- NIST SP 800-53 Revision 4 :: CM-5 (6)
- NIST SP 800-53 Revision 5 :: CM-5 (6)
- NIST SP 800-53A :: CM-5 (6).1

CIS Controls:

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

1.20 UBTU-22-232025 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must configure the `/var/log` directory to have mode `"755"` or less permissive.

```
ROUP ID: V-260488
RULE ID: SV-260488r958566
```

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, personally identifiable information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify the `/var/log` directory has mode of `"755"` or less permissive by using the following command:

Note: If `rsyslog` is active and enabled on the operating system, this requirement is not applicable.

```
$ stat -c "%n %a" /var/log
/var/log 755
```

If a value of `"755"` or less permissive is not returned, this is a finding.

Remediation:

Configure the `/var/log` directory to have permissions of `"0755"` by using the following command:







```
$ sudo chmod 0755 /var/log
```

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53 :: SI-11 c
- NIST SP 800-53 Revision 4 :: SI-11 b
- NIST SP 800-53 Revision 5 :: SI-11 b
- NIST SP 800-53A :: SI-11.1 (iv)

CIS Controls:

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

1.21 UBTU-22-232026 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.

```
GROUP ID: V-260489
RULE ID: SV-260489r958564
```

Rationale:

Any operating system providing too much information in error messages risks compromising the data and security of the structure, and content of error messages needs to be carefully considered by the organization.

Organizations carefully consider the structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information, such as account numbers, social security numbers, and credit card numbers.

The `/var/log/btmp`, `/var/log/wtmp`, and `/var/log/lastlog` files have group write and global read permissions to allow for the lastlog function to perform. Limiting the permissions beyond this configuration will result in the failure of functions that rely on the lastlog database.

Audit:

Verify the operating system has all system log files under the `/var/log` directory with a permission set to `"640"` or less permissive by using the following command:
Note: The `btmp`, `wtmp`, and `lastlog` files are excluded. Refer to the Discussion for details.

```
$ sudo find /var/log -perm /137 ! -name '*[bw]tmp' ! -name '*lastlog' -type f
-exec stat -c "%n %a" {} \;
```

If the command displays any output, this is a finding.

Remediation:

Configure the operating system to set permissions of all log files under the "/var/log" directory to "640" or more restricted by using the following command:

Note: The btmp, wtmp, and lastlog files are excluded. Refer to the Discussion for details.







```
$ sudo find /var/log -perm /137 ! -name '*[bw]tmp' ! -name '*lastlog' -type f  
-exec chmod 640 '{}' \;
```

Additional Information:

CCI-001312 Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited.

- NIST SP 800-53 :: SI-11 b
- NIST SP 800-53 Revision 4 :: SI-11 a
- NIST SP 800-53 Revision 5 :: SI-11 a
- NIST SP 800-53A :: SI-11.1 (iii)

CIS Controls:

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

1.22 UBTU-22-232027 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate system journal entries without revealing information that could be exploited by adversaries.

GROUP ID: V-260490 RULE ID: SV-260490r1069105
--

Rationale:

Any operating system providing too much information in error messages risks compromising the data and security of the structure, and content of error messages needs to be carefully considered by the organization.

Organizations carefully consider the structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information, such as account numbers, social security numbers, and credit card numbers.

Audit:

Verify the /run/log/journal and /var/log/journal directories have permissions set to "2750" or less permissive by using the following command:

```
$ sudo find /run/log/journal /var/log/journal -type d -exec stat -c "%n %a" {} \;
```

```
/run/log/journal 2750
/var/log/journal 2750
/var/log/journal/3b018e681c904487b11671b9c1987cce 2750
```

If any output returned has a permission set greater than "2750", this is a finding. Verify all files in the /run/log/journal and /var/log/journal directories have permissions set to "640" or less permissive by using the following command:

```
$ sudo find /run/log/journal /var/log/journal -type f -exec stat -c "%n %a" {} \;
```

```
/var/log/journal/3b018e681c904487b11671b9c1987cce/system@99dcc72bb1134aaeae4b
f157aa7606f4-00000000000003c7a-0006073f8d1c0fec.journal 640
/var/log/journal/3b018e681c904487b11671b9c1987cce/system.journal 640
/var/log/journal/3b018e681c904487b11671b9c1987cce/user-1000.journal 640
/var/log/journal/3b018e681c904487b11671b9c1987cce/user-
1000@bdeedf14602ff4081a77dc7a6debc8626-000000000000062a6-
00060b4b414b617a.journal 640
/var/log/journal/3b018e681c904487b11671b9c1987cce
```

If any output returned has a permission set greater than "640", this is a finding.

Remediation:

Configure the operating system to set the appropriate permissions to the files and directories used by the systemd journal:

Add or modify the following lines in the "/usr/lib/tmpfiles.d/systemd.conf" file:

```
z /run/log/journal 2750 root systemd-journal - -
Z /run/log/journal/%m ~2750 root systemd-journal - -
z /var/log/journal 2750 root systemd-journal - -
z /var/log/journal/%m 2750 root systemd-journal - -
z /var/log/journal/%m/system.journal 0750 root systemd-journal - -
```







Restart the system for the changes to take effect.

Additional Information:

CCI-001312 Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited.

- NIST SP 800-53 :: SI-11 b
- NIST SP 800-53 Revision 4 :: SI-11 a
- NIST SP 800-53 Revision 5 :: SI-11 a
- NIST SP 800-53A :: SI-11.1 (iii)

CIS Controls:

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

1.23 UBTU-22-232030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must configure `/var/log/syslog` file with mode `"640"` or less permissive.

```
GROUP ID: V-260491
RULE ID: SV-260491r958566
```

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, personally identifiable information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify that the operating system configures the `/var/log/syslog` file with mode `"640"` or less permissive by using the following command:

```
$ stat -c "%n %a" /var/log/syslog
/var/log/syslog 640
```

If a value of `"640"` or less permissive is not returned, this is a finding.

Remediation:

Configure the operating system to have permissions of `"640"` for the `/var/log/syslog` file by using the following command:







```
$ sudo chmod 0640 /var/log/syslog
```

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53 :: SI-11 c
- NIST SP 800-53 Revision 4 :: SI-11 b
- NIST SP 800-53 Revision 5 :: SI-11 b
- NIST SP 800-53A :: SI-11.1 (iv)

CIS Controls:

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

1.24 UBTU-22-232035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must configure audit tools with a mode of "755" or less permissive.

GROUP ID: V-260492 RULE ID: SV-260492r991557

Rationale:

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

Operating systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools and the corresponding rights the user enjoys in order to make access decisions regarding the access to audit tools.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Satisfies: SRG-OS-000256-GPOS-00097, SRG-OS-000257-GPOS-00098

Audit:

Verify the operating system configures the audit tools to have a file permission of "755" or less to prevent unauthorized access by using the following command:

```
$ stat -c "%n %a" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace  
/sbin/auditd /sbin/audispd* /sbin/augenrules  
  
/sbin/auditctl 755  
/sbin/aureport 755  
/sbin/ausearch 755  
/sbin/autrace 755  
/sbin/auditd 755  
/sbin/audispd-zos-remote 755  
/sbin/augenrules 755
```

If any of the audit tools have a mode more permissive than "0755", this is a finding.

Remediation:

Configure the audit tools on the operating system to be protected from unauthorized access by setting the correct permissive mode using the following command:

```
$ sudo chmod 755 <audit_tool_name>
```

Replace "<audit_tool_name>" with the audit tool that does not have the correct permissions.

References:

1. CIS Recommendation "Ensure audit tools mode is configured"

Additional Information:







CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9
- NIST SP 800-53A :: AU-9.1

CIS Controls:

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

1.25 UBTU-22-232040 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must have directories that contain system commands owned by "root".

```
GROUP ID: V-260493
RULE ID: SV-260493r991559
```

Rationale:

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

Operating systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools and the corresponding rights the user has in order to make access decisions regarding the deletion of audit tools.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Audit:

Verify the system commands directories are owned by "root" by using the following command:

```
$ sudo find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -
user root -type d -exec stat -c "%n %U" '{}' \;
```

If any system commands directories are returned, this is a finding.

Remediation:

Configure the operating system commands directories to be protected from unauthorized access. Run the following command:







```
$ sudo find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -
user root -type d -exec chown root '{}' \;
```

Additional Information:

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9
- NIST SP 800-53A :: AU-9.1

CIS Controls:

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

1.26 UBTU-22-232045 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must have directories that contain system commands group-owned by "root".

```
GROUP ID: V-260494
RULE ID: SV-260494r991559
```

Rationale:

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

Operating systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools and the corresponding rights the user has in order to make access decisions regarding the deletion of audit tools.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Audit:

Verify the system commands directories are group-owned by "root" by using the following command:

```
$ sudo find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -group root -type d -exec stat -c "%n %G" '{}' \;
```

If any system commands directories are returned that are not Set Group ID up on execution (SGID) files and owned by a privileged account, this is a finding.

Remediation:

Configure the operating system commands directories to be protected from unauthorized access. Run the following command:







```
$ sudo find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -group root -type d -exec chgrp root '{}' \;
```

Additional Information:

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9
- NIST SP 800-53A :: AU-9.1

CIS Controls:

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

1.27 UBTU-22-232050 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must have system commands owned by "root" or a system account.

```
GROUP ID: V-260495
RULE ID: SV-260495r991560
```

Rationale:

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to the operating system with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system commands contained in the following directories are owned by "root", or a required system account, by using the following command:

```
$ sudo find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -
user root -type f -exec stat -c "%n %U" '{}' \;
```

If any system commands are returned and are not owned by a required system account, this is a finding.

Remediation:

Configure the operating system commands and their respective parent directories to be protected from unauthorized access. Run the following command, replacing "<command_name>" with any system command not owned by "root" or a required system account:







```
$ sudo chown root <command_name>
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53 :: CM-5 (6)
- NIST SP 800-53 Revision 4 :: CM-5 (6)
- NIST SP 800-53 Revision 5 :: CM-5 (6)
- NIST SP 800-53A :: CM-5 (6).1

CIS Controls:

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

1.28 UBTU-22-232055 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must have system commands group-owned by "root" or a system account.

```
GROUP ID: V-260496
RULE ID: SV-260496r991560
```

Rationale:

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to the operating system with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system commands contained in the following directories are group-owned by "root" or a required system account by using the following command:

```
$ sudo find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin !
-group root -type f ! -perm /2000 -exec stat -c "%n %G" '{} ' \;
```

If any system commands are returned that are not Set Group ID upon execution (SGID) files and group-owned by a required system account, this is a finding.

Remediation:

Configure the operating system commands to be protected from unauthorized access. Run the following command, replacing "<command_name>" with any system command not group-owned by "root" or a required system account:







```
$ sudo chgrp root <command_name>
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53 :: CM-5 (6)
- NIST SP 800-53 Revision 4 :: CM-5 (6)
- NIST SP 800-53 Revision 5 :: CM-5 (6)
- NIST SP 800-53A :: CM-5 (6).1

CIS Controls:

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

1.29 UBTU-22-232060 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system library directories must be owned by "root".

```
GROUP ID: V-260497
RULE ID: SV-260497r991560
```

Rationale:

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the systemwide shared library directories "/lib", "/lib64", and "/usr/lib" are owned by "root" by using the following command:

```
$ sudo find /lib /usr/lib /lib64 ! -user root -type d -exec stat -c "%n %U"
'{}' \;
```

If any systemwide library directory is returned, this is a finding.

Remediation:

Configure the library files and their respective parent directories to be protected from unauthorized access. Run the following command:







```
$ sudo find /lib /usr/lib /lib64 ! -user root -type d -exec chown root '{}'
\;
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53 :: CM-5 (6)
- NIST SP 800-53 Revision 4 :: CM-5 (6)
- NIST SP 800-53 Revision 5 :: CM-5 (6)
- NIST SP 800-53A :: CM-5 (6).1

CIS Controls:

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

1.30 UBTU-22-232065 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system library directories must be group-owned by "root".

```
GROUP ID: V-260498
RULE ID: SV-260498r991560
```

Rationale:

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the systemwide library directories "/lib", "/lib64", and "/usr/lib" are group-owned by "root" by using the following command:

```
$ sudo find /lib /usr/lib /lib64 ! -group root -type d -exec stat -c "%n %G"
'{}' \;
```

If any systemwide shared library directory is returned, this is a finding.

Remediation:

Configure the operating system library directories to be protected from unauthorized access. Run the following command:







```
$ sudo find /lib /usr/lib /lib64 ! -group root -type d -exec chgrp root '{}'
\;
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53 :: CM-5 (6)
- NIST SP 800-53 Revision 4 :: CM-5 (6)
- NIST SP 800-53 Revision 5 :: CM-5 (6)
- NIST SP 800-53A :: CM-5 (6).1

CIS Controls:

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

1.31 UBTU-22-232070 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system library files must be owned by "root".

```
GROUP ID: V-260499
RULE ID: SV-260499r991560
```

Rationale:

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the systemwide shared library files contained in the directories "/lib", "/lib64", and "/usr/lib" are owned by "root" by using the following command:

```
$ sudo find /lib /usr/lib /lib64 ! -user root -type f -exec stat -c "%n %U"
'{}' \;
```

If any systemwide library file is returned, this is a finding.

Remediation:

Configure the operating system library files to be protected from unauthorized access. Run the following command:







```
$ sudo find /lib /usr/lib /lib64 ! -user root -type f -exec chown root '{}'
\;
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53 :: CM-5 (6)
- NIST SP 800-53 Revision 4 :: CM-5 (6)
- NIST SP 800-53 Revision 5 :: CM-5 (6)
- NIST SP 800-53A :: CM-5 (6).1

CIS Controls:

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

1.32 UBTU-22-232075 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system library files must be group-owned by "root".

```
GROUP ID: V-260500  
RULE ID: SV-260500r1069099
```

Rationale:

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the systemwide library files contained in the directories "/lib", "/lib64", and "/usr/lib" are group-owned by "root", or a required system account, by using the following command:

```
$ sudo find /lib /lib64 /usr/lib /usr/lib64 ! -group root -type f -exec stat  
-c "%n %G" '{}' \;
```

If any systemwide shared library file is returned and is not group-owned by a required system account, this is a finding.

Remediation:

Configure the operating system library files to be protected from unauthorized access. Run the following command, replacing "<command_name>" with any system command not group-owned by "root" or a required system account:







```
$ sudo chgrp root <command_name>
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53 :: CM-5 (6)
- NIST SP 800-53 Revision 4 :: CM-5 (6)
- NIST SP 800-53 Revision 5 :: CM-5 (6)
- NIST SP 800-53A :: CM-5 (6).1

CIS Controls:

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

1.33 UBTU-22-232080 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must configure the directories used by the system journal to be owned by "root".

GROUP ID: V-260501
RULE ID: SV-260501r958566

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, personally identifiable information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify the /run/log/journal and /var/log/journal directories are owned by "root" by using the following command:

```
$ sudo find /run/log/journal /var/log/journal -type d -exec stat -c "%n %U" {} \;  
  
/run/log/journal root  
/var/log/journal root  
/var/log/journal/3b018e681c904487b11671b9c1987cce root
```

If any output returned is not owned by "root", this is a finding.

Remediation:

Configure the operating system to set the appropriate ownership to the directories used by the systemd journal:

Add or modify the following lines in the "/usr/lib/tmpfiles.d/systemd.conf" file:

```
z /run/log/journal 2640 root systemd-journal - -  
z /var/log/journal 2640 root systemd-journal - -
```







Restart the system for the changes to take effect.

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53 :: SI-11 c
- NIST SP 800-53 Revision 4 :: SI-11 b
- NIST SP 800-53 Revision 5 :: SI-11 b
- NIST SP 800-53A :: SI-11.1 (iv)

CIS Controls:

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

1.34 UBTU-22-232085 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must configure the directories used by the system journal to be group-owned by "systemd-journal".

GROUP ID: V-260502
RULE ID: SV-260502r958566

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, personally identifiable information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify the /run/log/journal and /var/log/journal directories are group-owned by "systemd-journal" by using the following command:

```
$ sudo find /run/log/journal /var/log/journal -type d -exec stat -c "%n %G" {} \;
```

/run/log/journal systemd-journal
/var/log/journal systemd-journal
/var/log/journal/3b018e681c904487b11671b9c1987cce systemd-journal

If any output returned is not group-owned by "systemd-journal", this is a finding.

Remediation:

Configure the operating system to set the appropriate group-ownership to the directories used by the systemd journal:

Add or modify the following lines in the "/usr/lib/tmpfiles.d/systemd.conf" file:

```
z /run/log/journal 2640 root systemd-journal - -  
z /var/log/journal 2640 root systemd-journal - -
```







Restart the system for the changes to take effect.

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53 :: SI-11 c
- NIST SP 800-53 Revision 4 :: SI-11 b
- NIST SP 800-53 Revision 5 :: SI-11 b
- NIST SP 800-53A :: SI-11.1 (iv)

CIS Controls:

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

1.35 UBTU-22-232090 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must configure the files used by the system journal to be owned by "root".

GROUP ID: V-260503
RULE ID: SV-260503r958566

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, personally identifiable information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify the /run/log/journal and /var/log/journal files are owned by "root" by using the following command:

```
$ sudo find /run/log/journal /var/log/journal -type f -exec stat -c "%n %U" {} \;
```

/var/log/journal/3b018e681c904487b11671b9c1987cce/system@99dcc72bb1134aaeae4bf157aa7606f4-00000000000003c7a-0006073f8d1c0fec.journal root
/var/log/journal/3b018e681c904487b11671b9c1987cce/system.journal root
/var/log/journal/3b018e681c904487b11671b9c1987cce/user-1000.journal root
/var/log/journal/3b018e681c904487b11671b9c1987cce/user-1000@bde9df14602ff4081a77dc7a6debc8626-000000000000062a6-00060b4b414b617a.journal root
/var/log/journal/3b018e681c904487b11671b9c1987cce/system@99dcc72bb1134aaeae4bf157aa7606f4-00000000000005301-000609a409593.journal root
/var/log/journal/3b018e681c904487b11671b9c1987cce/system@99dcc72bb1134aaeae4bf157aa7606f4-0000000000000001-000604dae53225ee.journal root
/var/log/journal/3b018e681c904487b11671b9c1987cce/user-1000@bde9df14602ff4081a77dc7a6debc8626-0000000000000083b-000604dae72c7e3b.journal root

If any output returned is not owned by "root", this is a finding.

Remediation:

Configure the operating system to set the appropriate ownership to the files used by the systemd journal:

Add or modify the following lines in the "/usr/lib/tmpfiles.d/systemd.conf" file:

```
z /run/log/journal/%m ~2640 root systemd-journal - -
z /var/log/journal/%m 2640 root systemd-journal - -
z /var/log/journal/%m/system.journal 0640 root systemd-journal - -
```







Restart the system for the changes to take effect.

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53 :: SI-11 c
- NIST SP 800-53 Revision 4 :: SI-11 b
- NIST SP 800-53 Revision 5 :: SI-11 b
- NIST SP 800-53A :: SI-11.1 (iv)

CIS Controls:

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

1.36 UBTU-22-232095 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must configure the files used by the system journal to be group-owned by "systemd-journal".

GROUP ID: V-260504 RULE ID: SV-260504r958566

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, personally identifiable information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify the /run/log/journal and /var/log/journal files are group-owned by "systemd-journal" by using the following command:

```
$ sudo find /run/log/journal /var/log/journal -type f -exec stat -c "%n %G" {} \;
```

/var/log/journal/3b018e681c904487b11671b9c1987cce/system@99dcc72bb1134aaeae4bf157aa7606f4-00000000000003c7a-0006073f8d1c0fec.journal systemd-journal
/var/log/journal/3b018e681c904487b11671b9c1987cce/system.journal systemd-journal
/var/log/journal/3b018e681c904487b11671b9c1987cce/user-1000.journal systemd-journal
/var/log/journal/3b018e681c904487b11671b9c1987cce/user-1000@bde9df14602ff4081a77dc7a6debc8626-000000000000062a6-00060b4b414b617a.journal systemd-journal
/var/log/journal/3b018e681c904487b11671b9c1987cce/system@99dcc72bb1134aaeae4bf157aa7606f4-00000000000005301-000609a409593.journal systemd-journal
/var/log/journal/3b018e681c904487b11671b9c1987cce/system@99dcc72bb1134aaeae4bf157aa7606f4-0000000000000001-000604dae53225ee.journal systemd-journal
/var/log/journal/3b018e681c904487b11671b9c1987cce/user-1000@bde9df14602ff4081a77dc7a6debc8626-000000000000083b-000604dae72c7e3b.journal systemd-journal

If any output returned is not group-owned by "systemd-journal", this is a finding.

Remediation:

Configure the operating system to set the appropriate group-ownership to the files used by the systemd journal:

Add or modify the following line in the "/usr/lib/tmpfiles.d/systemd.conf" file:

```
z /run/log/journal/%m ~2640 root systemd-journal - -
z /var/log/journal/%m 2640 root systemd-journal - -
z /var/log/journal/%m/system.journal 0640 root systemd-journal - -
```







Restart the system for the changes to take effect.

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53 :: SI-11 c
- NIST SP 800-53 Revision 4 :: SI-11 b
- NIST SP 800-53 Revision 5 :: SI-11 b
- NIST SP 800-53A :: SI-11.1 (iv)

CIS Controls:

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

1.37 UBTU-22-232100 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must be configured so that the "journalctl" command is owned by "root".

```
GROUP ID: V-260505  
RULE ID: SV-260505r958566
```

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, Personally identifiable information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify that the "journalctl" command is owned by "root" by using the following command:

```
$ sudo find /usr/bin/journalctl -exec stat -c "%n %U" {} \;  
  
/usr/bin/journalctl root
```

If "journalctl" is not owned by "root", this is a finding.

Remediation:

Configure "journalctl" to be owned by "root":







```
$ sudo chown root /usr/bin/journalctl
```

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53 :: SI-11 c
- NIST SP 800-53 Revision 4 :: SI-11 b
- NIST SP 800-53 Revision 5 :: SI-11 b
- NIST SP 800-53A :: SI-11.1 (iv)

CIS Controls:

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

1.38 UBTU-22-232105 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must be configured so that the "journalctl" command is group-owned by "root".

```
GROUP ID: V-260506  
RULE ID: SV-260506r958566
```

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, personally identifiable information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify that the "journalctl" command is group-owned by "root" by using the following command:

```
$ sudo find /usr/bin/journalctl -exec stat -c "%n %G" {} \;  
  
/usr/bin/journalctl root
```

If "journalctl" is not group-owned by "root", this is a finding.

Remediation:

Configure "journalctl" to be group-owned by "root":







```
$ sudo chown :root /usr/bin/journalctl
```

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53 :: SI-11 c
- NIST SP 800-53 Revision 4 :: SI-11 b
- NIST SP 800-53 Revision 5 :: SI-11 b
- NIST SP 800-53A :: SI-11.1 (iv)

CIS Controls:

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

1.39 UBTU-22-232110 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must configure audit tools to be owned by "root".

GROUP ID: V-260507
RULE ID: SV-260507r991557

Rationale:

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

Operating systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools and the corresponding rights the user enjoys in order to make access decisions regarding the access to audit tools.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Satisfies: SRG-OS-000256-GPOS-00097, SRG-OS-000257-GPOS-00098

Audit:

Verify the operating system configures the audit tools to be owned by "root" to prevent any unauthorized access with the following command:

```
$ stat -c "%n %U" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace  
/sbin/auditd /sbin/audispd* /sbin/augenrules  
  
/sbin/auditctl root  
/sbin/aureport root  
/sbin/ausearch root  
/sbin/autrace root  
/sbin/auditd root  
/sbin/audispd-zos-remote root  
/sbin/augenrules root
```

If any of the audit tools are not owned by "root", this is a finding.

Remediation:

Configure the audit tools on the operating system to be protected from unauthorized access by setting the file owner as root using the following command:

```
$ sudo chown root <audit_tool_name>
```

Replace "<audit_tool_name>" with each audit tool not owned by "root".

References:

1. CIS Recommendation "Ensure audit tools owner is configured"

Additional Information:







CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9
- NIST SP 800-53A :: AU-9.1

CIS Controls:

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

1.40 UBTU-22-232120 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must configure the "/var/log" directory to be owned by "root".

```
GROUP ID: V-260508  
RULE ID: SV-260508r958566
```

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, personally identifiable information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify the operating system configures the "/var/log" directory to be owned by "root" by using the following command:

```
$ stat -c "%n %U" /var/log  
  
/var/log root
```

If the "/var/log" directory is not owned by "root", this is a finding.

Remediation:

Configure the operating system to have root own the "/var/log" directory by using the following command:







```
$ sudo chown root /var/log
```

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53 :: SI-11 c
- NIST SP 800-53 Revision 4 :: SI-11 b
- NIST SP 800-53 Revision 5 :: SI-11 b
- NIST SP 800-53A :: SI-11.1 (iv)

CIS Controls:

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

1.41 UBTU-22-232125 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must configure the "/var/log" directory to be group-owned by "syslog".

```
GROUP ID: V-260509  
RULE ID: SV-260509r958566
```

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, personally identifiable information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify that the operating system configures the "/var/log" directory to be group-owned by "syslog" by using the following command:

```
$ stat -c "%n %G" /var/log  
  
/var/log syslog
```

If the "/var/log" directory is not group-owned by "syslog", this is a finding.

Remediation:

Configure the operating system to have syslog group-own the "/var/log" directory by using the following command:







```
$ sudo chgrp syslog /var/log
```

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53 :: SI-11 c
- NIST SP 800-53 Revision 4 :: SI-11 b
- NIST SP 800-53 Revision 5 :: SI-11 b
- NIST SP 800-53A :: SI-11.1 (iv)

CIS Controls:

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

1.42 UBTU-22-232130 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must configure `/var/log/syslog` file to be owned by `syslog`.

```
GROUP ID: V-260510
RULE ID: SV-260510r958566
```

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, personally identifiable information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify that the operating system configures the `/var/log/syslog` file to be owned by `syslog` by using the following command:

```
$ stat -c "%n %U" /var/log/syslog
/var/log/syslog
```

If the `/var/log/syslog` file is not owned by `syslog`, this is a finding.

Remediation:

Configure the operating system to have `syslog` own the `/var/log/syslog` file by using the following command:







```
$ sudo chown syslog /var/log/syslog
```

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53 :: SI-11 c
- NIST SP 800-53 Revision 4 :: SI-11 b
- NIST SP 800-53 Revision 5 :: SI-11 b
- NIST SP 800-53A :: SI-11.1 (iv)

CIS Controls:

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

1.43 UBTU-22-232135 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must configure the "/var/log/syslog" file to be group-owned by "adm".

```
GROUP ID: V-260511  
RULE ID: SV-260511r958566
```

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, personally identifiable information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify that the operating system configures the "/var/log/syslog" file to be group-owned by "adm" by using the following command:

```
$ stat -c "%n %G" /var/log/syslog  
  
/var/log/syslog adm
```

If the "/var/log/syslog" file is not group-owned by "adm", this is a finding.

Remediation:

Configure the operating system to have adm group-own the "/var/log/syslog" file by using the following command:







```
$ sudo chgrp adm /var/log/syslog
```

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53 :: SI-11 c
- NIST SP 800-53 Revision 4 :: SI-11 b
- NIST SP 800-53 Revision 5 :: SI-11 b
- NIST SP 800-53A :: SI-11.1 (iv)

CIS Controls:

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

1.44 UBTU-22-232140 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must be configured so that the "journalctl" command is not accessible by unauthorized users.

```
GROUP ID: V-260512  
RULE ID: SV-260512r958564
```

Rationale:

Any operating system providing too much information in error messages risks compromising the data and security of the structure, and content of error messages needs to be carefully considered by the organization.

Organizations carefully consider the structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information, such as account numbers, social security numbers, and credit card numbers.

Audit:

Verify that the "journalctl" command has a permission set of "740" by using the following command:

```
$ sudo find /usr/bin/journalctl -exec stat -c "%n %a" {} \;  
  
/usr/bin/journalctl 740
```

If "journalctl" is not set to "740", this is a finding.

Remediation:

Configure "journalctl" to have a permission set of "740":







```
$ sudo chmod 740 /usr/bin/journalctl
```

Additional Information:

CCI-001312 Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited.

- NIST SP 800-53 :: SI-11 b
- NIST SP 800-53 Revision 4 :: SI-11 a
- NIST SP 800-53 Revision 5 :: SI-11 a
- NIST SP 800-53A :: SI-11.1 (iii)

CIS Controls:

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

1.45 UBTU-22-232145 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must set a sticky bit on all public directories to prevent unauthorized and unintended information transferred via shared system resources.

```
GROUP ID: V-260513
RULE ID: SV-260513r958524
```

Rationale:

Preventing unauthorized information transfers mitigates the risk of information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection.

This requirement generally applies to the design of an information technology product, but it can also apply to the configuration of particular information system components that are, or use, such products. This can be verified by acceptance/validation processes in DOD or other government agencies.

There may be shared resources with configurable protections (e.g., files in storage) that may be assessed on specific information system components.

Audit:

Verify that all public directories have the public sticky bit set by using the following command:

```
$ sudo find / -type d -perm -002 ! -perm -1000
```

If any public directories are found missing the sticky bit, this is a finding.

Remediation:

Configure all public directories to have the sticky bit set to prevent unauthorized and unintended information transferred via shared system resources.

Set the sticky bit on all public directories using the following command, replacing "<public_directory_name>" with any directory path missing the sticky bit:

```
$ sudo chmod +t <public_directory_name>
```

References:







1. CIS Recommendation "Ensure world writable files and directories are secured"

Additional Information:

CCI-001090 Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53 :: SC-4
- NIST SP 800-53 Revision 4 :: SC-4
- NIST SP 800-53 Revision 5 :: SC-4
- NIST SP 800-53A :: SC-4.1

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.46 UBTU-22-251010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must have an application firewall installed in order to control remote access methods.

```
GROUP ID: V-260514
RULE ID: SV-260514r958672
```

Rationale:

Remote access services, such as those providing remote access to network devices and information systems, which lack automated control capabilities, increase risk and make remote user access management difficult at best.

Remote access is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

The operating system functionality (e.g., RDP) must be capable of taking enforcement action if the audit reveals unauthorized activity. Automated control of remote access sessions allows organizations to ensure ongoing compliance with remote access policies by enforcing connection rules of remote access applications on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

Audit:

Verify that the Uncomplicated Firewall is installed by using the following command:

```
$ dpkg -l | grep ufw

ii      ufw      0.36.1-4ubuntu0.1      all      program for managing a Netfilter
firewall
```

If the "ufw" package is not installed, ask the system administrator if another application firewall is installed.

If no application firewall is installed, this is a finding.

Remediation:

Install the Uncomplicated Firewall by using the following command:

```
$ sudo apt-get install ufw
```

References:







1. CIS Recommendation "Ensure ufw is installed"

Additional Information:

CCI-002314 Employ automated mechanisms to control remote access methods.

- NIST SP 800-53 Revision 4 :: AC-17 (1)
- NIST SP 800-53 Revision 5 :: AC-17 (1)v

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

1.47 UBTU-22-251015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must enable and run the Uncomplicated Firewall (ufw).

```
GROUP ID: V-260515  
RULE ID: SV-260515r958672
```

Rationale:

Remote access services, such as those providing remote access to network devices and information systems, which lack automated control capabilities, increase risk and make remote user access management difficult at best.

Remote access is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

The operating system functionality (e.g., RDP) must be capable of taking enforcement action if the audit reveals unauthorized activity. Automated control of remote access sessions allows organizations to ensure ongoing compliance with remote access policies by enforcing connection rules of remote access applications on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

Audit:

Verify the ufw is enabled on the system with the following command:

```
$ sudo ufw status  
  
Status: active
```

If the above command returns the status as "inactive" or any type of error, this is a finding.

Remediation:

Enable the ufw by using the following command:

```
$ sudo ufw enable
```

References:







1. CIS Recommendation "Ensure ufw service is enabled"

Additional Information:

CCI-002314 Employ automated mechanisms to control remote access methods.

- NIST SP 800-53 Revision 4 :: AC-17 (1)
- NIST SP 800-53 Revision 5 :: AC-17 (1)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

1.48 UBTU-22-251020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must have an application firewall enabled.

```
GROUP ID: V-260516  
RULE ID: SV-260516r991593
```

Rationale:

Firewalls protect computers from network attacks by blocking or limiting access to open network ports. Application firewalls limit which applications are allowed to communicate over the network.

Audit:

Verify the Uncomplicated Firewall (ufw) is enabled on the system with the following command:

```
$ systemctl status ufw.service | grep -i "active:"  
  
Active: active (exited) since Thu 2022-12-25 00:00:01 NZTD; 365 days 11h ago
```

If "ufw.service" is "inactive", this is a finding.

If the ufw is not installed, ask the system administrator if another application firewall is installed. If no application firewall is installed, this is a finding.

Remediation:

Enable and start the ufw by using the following command:

```
$ sudo systemctl enable ufw.service --now
```

References:







1. CIS Recommendation "Ensure ufw is enabled"

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

1.49 UBTU-22-251025 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must configure the Uncomplicated Firewall (ufw) to rate-limit impacted network interfaces.

GROUP ID: V-260517
RULE ID: SV-260517r958902

Rationale:

Denial of service (DoS) is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

This requirement addresses the configuration of the operating system to mitigate the impact of DoS attacks that have occurred or are ongoing on system availability. For each system, known and potential DoS attacks must be identified and solutions for each type implemented. A variety of technologies exist to limit or, in some cases, eliminate the effects of DoS attacks (e.g., limiting processes or establishing memory partitions). Employing increased capacity and bandwidth, combined with service redundancy, may reduce the susceptibility to some DoS attacks.

Audit:

Verify an application firewall is configured to rate limit any connection to the system. Check all the services listening to the ports by using the following command:

```
$ ss -l46ut
```

Netid	State	Recv-Q	Send-Q	Process
Local Address:Port	Peer Address:Port			
tcp	LISTEN	0		511
*:http			*:*	
tcp	LISTEN	0		128
[::]:ssh			[::]:*	
tcp	LISTEN	0		128
[::]:ipp			[::]:*	
tcp	LISTEN	0		128
[::]:smtp			[::]:*	

For each entry, verify that the ufw is configured to rate limit the service ports by using the following command:

```
$ sudo ufw status
```

```
Status: active
```

To		Action	From
--		-----	----
80/tcp		LIMIT	Anywhere
25/tcp		LIMIT	Anywhere
Anywhere	DENY		240.9.19.81
443		LIMIT	Anywhere
22/tcp		LIMIT	Anywhere
80/tcp (v6)	LIMIT		Anywhere
25/tcp (v6)	LIMIT		Anywhere
22/tcp (v6)	LIMIT		Anywhere (v6)
25		DENY OUT	Anywhere
25 (v6)		DENY OUT	Anywhere (v6)

If any port with a state of "LISTEN" that does not have an action of "DENY", is not marked with the "LIMIT" action, this is a finding.

Remediation:

Configure the application firewall to protect against or limit the effects of DoS attacks by ensuring the operating system is implementing rate-limiting measures on impacted network interfaces.

For each service with a port listening to connections, run the following command, replacing "<service_name>" with the service that needs to be rate limited.

```
$ sudo ufw limit <service_name>
```

Rate-limiting can also be done on an interface. An example of adding a rate limit on the "ens160" interface follows:







```
$ sudo ufw limit in on ens160
```

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial of service events.

- NIST SP 800-53 Revision 4 :: SC-5
- NIST SP 800-53 Revision 5 :: SC-5 a

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

1.50 UBTU-22-251030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must be configured to prohibit or restrict the use of functions, ports, protocols, and/or services, as defined in the PPSM CAL and vulnerability assessments.

GROUP ID: V-260518 RULE ID: SV-260518r958480

Rationale:

To prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary physical and logical ports/protocols on information systems.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., VPN and IPS); however, doing so increases risk over limiting the services provided by any one component.

To support the requirements and principles of least functionality, the operating system must support the organizational requirements, providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved to conduct official business or to address authorized quality of life issues.

Audit:

Check the firewall configuration for any unnecessary or prohibited functions, ports, protocols, and/or services by using the following command:

```
$ sudo ufw show raw

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts      bytes target      prot opt in      out      source
destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts      bytes target      prot opt in      out      source
destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts      bytes target      prot opt in      out      source
destination
```

Ask the system administrator for the site or program PPSM CLSA. Verify the services allowed by the firewall match the PPSM CLSA.

If there are any additional ports, protocols, or services that are not included in the PPSM CLSA, this is a finding.

If there are any ports, protocols, or services that are prohibited by the PPSM CAL, this is a finding.

Remediation:

Add all ports, protocols, or services allowed by the PPSM CLSA by using the following command:

```
$ sudo ufw allow <direction> <port/protocol/service>
```

Where the direction is "in" or "out" and the port is the one corresponding to the protocol or service allowed.

To deny access to ports, protocols, or services, use:







```
$ sudo ufw deny <direction> <port/protocol/service>
```

Additional Information:

CCI-000382 Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 b
- NIST SP 800-53 Revision 5 :: CM-7 b
- NIST SP 800-53A :: CM-7.1 (iii)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

1.51 UBTU-22-252010 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must, for networked systems, compare internal information system clocks at least every 24 hours with a server synchronized to one of the redundant United States Naval Observatory (USNO) time servers, or a time server designated for the appropriate DOD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS).

```
GROUP ID: V-260519
RULE ID: SV-260519r1038944
```

Rationale:

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Synchronizing internal information system clocks provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

Organizations should consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

Note that USNO offers authenticated NTP service to DOD and U.S. Government agencies operating on the NIPR and SIPR networks. Visit <https://www.usno.navy.mil/USNO/time/ntp/DOD-customers> for more information.

Audit:

Verify the operating system is configured to compare the system clock at least every 24 hours to the authoritative time source by using the following command:

Note: If the system is not networked, this requirement is not applicable.

```
$ sudo grep maxpoll -ir /etc/chrony*

server tick.usno.navy.mil iburst maxpoll 16
```

If the "maxpoll" option is set to a number greater than 16, the line is commented out, or is missing, this is a finding.

Verify that the "chrony.conf" file is configured to an authoritative DOD time source by using the following command:

```
$ sudo grep -ir server /etc/chrony*

server tick.usno.navy.mil iburst maxpoll 16
server tock.usno.navy.mil iburst maxpoll 16
server ntp2.usno.navy.mil iburst maxpoll 16
```

If "server" is not defined, is not set to an authoritative DOD time source, is commented out, or missing, this is a finding.

Remediation:

Configure the operating system to compare the system clock at least every 24 hours to the authoritative time source.

Add or modify the following line in the "/etc/chrony/chrony.conf" file:

```
server [source] iburst maxpoll = 16
```

Restart "chrony.service" for the changes to take effect by using the following command:

```
$ sudo systemctl restart chrony.service
```

Additional Information:





CCI-004923 Compare the internal system clocks on an organization-defined frequency with organization-defined authoritative time source.

- NIST SP 800-53 Revision 5 :: SC-45 (1) (a)

CCI-001891 The information system compares internal information system clocks on an organization-defined frequency with an organization-defined authoritative time source.

- NIST SP 800-53 Revision 4 :: AU-8 (1) (a)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 <u>Standardize Time Synchronization</u> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.			
v7	6.1 <u>Utilize Three Synchronized Time Sources</u> Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.			

1.52 UBTU-22-252015 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must synchronize internal information system clocks to the authoritative time source when the time difference is greater than one second.

```
GROUP ID: V-260520
RULE ID: SV-260520r1044776
```

Rationale:

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events.

Synchronizing internal information system clocks provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network. Organizations should consider setting time periods for different types of systems (e.g., financial, legal, or mission-critical systems).

Organizations should also consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints). This requirement is related to the comparison done every 24 hours in SRG-OS-000355 because a comparison must be done to determine the time difference.

Audit:

Verify the operating system synchronizes internal system clocks to the authoritative time source when the time difference is greater than one second.

Note: If the system is not networked, this requirement is not applicable.

Check the value of "makestep" by using the following command:

```
$ grep -ir makestep /etc/chrony*

makestep 1 -1
```

If "makestep" is not set to "1 -1", is commented out, or is missing, this is a finding. Verify the NTP service is active and the system clock is synchronized with the authoritative time source:

```
$ timedatectl | grep -Ei '(synchronized|service)'

System clock synchronized: yes
NTP service: active
```

If the NTP service is not active, this is a finding.

If the system clock is not synchronized, this is a finding.

Remediation:

Configure chrony to synchronize the internal system clocks to the authoritative source when the time difference is greater than one second by doing the following:

Edit the "/etc/chrony/chrony.conf" file and add:

```
makestep 1 -1
```

Restart the chrony service:

```
$ sudo systemctl restart chrony.service
```

Additional Information:

CCI-004926 Synchronize the internal system clocks to the authoritative time source when the time difference is greater than organization-defined time period.

- NIST SP 800-53 Revision 5 :: SC-45 (1) (b)

CCI-002046 The information system synchronizes the internal system clocks to the authoritative time source when the time difference is greater than the organization-defined time period.

- NIST SP 800-53 Revision 4 :: AU-8 (1) (b)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 Standardize Time Synchronization Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	6.1 Utilize Three Synchronized Time Sources Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

1.53 UBTU-22-252020 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC).

```
GROUP ID: V-260521  
RULE ID: SV-260521r958788
```

Rationale:

If time stamps are not consistently applied and there is no common time reference, it is difficult to perform forensic analysis.

Time stamps generated by the operating system include date and time. Time is commonly expressed in UTC or local time with an offset from UTC.

Audit:

Verify the time zone is configured to use UTC by using the following command:

```
$ timedatectl status | grep -i "time zone"  
  
Time zone: Etc/UTC (UTC, +0000)
```

If "Time zone" is not set to UTC, this is a finding.

Remediation:

To Configure the operating system time zone to use UTC, run the following command:

```
$ sudo timedatectl set-timezone Etc/UTC
```

Additional Information:

CCI-001890 Record time stamps for audit records that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

- NIST SP 800-53 Revision 4 :: AU-8 b
- NIST SP 800-53 Revision 5 :: AU-8 b

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 <u>Standardize Time Synchronization</u> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	6.1 <u>Utilize Three Synchronized Time Sources</u> Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

1.54 UBTU-22-253010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must be configured to use TCP syncookies.

```
GROUP ID: V-260522
RULE ID: SV-260522r1069097
```

Rationale:

DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

Managing excess capacity ensures that sufficient capacity is available to counter flooding attacks. Employing increased capacity and service redundancy may reduce the susceptibility to some DoS attacks. Managing excess capacity may include, for example, establishing selected usage priorities, quotas, or partitioning.

Audit:

Verify the operating system is configured to use TCP syncookies by using the following command:

```
$ sysctl net.ipv4.tcp_syncookies

net.ipv4.tcp_syncookies = 1
```

If the value is not "1", this is a finding.

Check the saved value of TCP syncookies by using the following command:

```
$ sudo grep -ir net.ipv4.tcp_syncookies /etc/sysctl.d/*.conf
/run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf /etc/sysctl.conf 2> /dev/null
```

If the "net.ipv4.tcp_syncookies" option is not set to "1", is commented out, or is missing, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure the operating system to use TCP syncookies by using the following command:

```
$ sudo sysctl -w net.ipv4.tcp_syncookies=1
```

If "1" is not the system's default value, add or update the following line in "/etc/sysctl.conf":

```
net.ipv4.tcp_syncookies =
```

References:





1. CIS Recommendation "Ensure tcp syn cookies is enabled"

Additional Information:

CCI-001095 Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.

- NIST SP 800-53 :: SC-5 (2)
- NIST SP 800-53 Revision 4 :: SC-5 (2)
- NIST SP 800-53 Revision 5 :: SC-5 (2)
- NIST SP 800-53A :: SC-5 (2).1

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

1.55 UBTU-22-255010 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

The operating system must have SSH installed.

GROUP ID: V-260523
RULE ID: SV-260523r958908

Rationale:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

Audit:

Verify the SSH package is installed by using the following command:

```
$ sudo dpkg -l | grep openssh

ii      openssh-client      1:8.9p1-3ubuntu0.4      amd64      secure shell (SSH)
client, for secure access to remote machines

ii      openssh-server         1:8.9p1-3ubuntu0.4      amd64      secure shell (SSH)
server, for secure access from remote machines

ii      openssh-sftp-server     1:8.9p1-3ubuntu0.4      amd64      secure shell
(SSH) sftp server module, for SFTP access from remote machines
```

If the "openssh" server package is not installed, this is a finding.

Remediation:

Install the "ssh" meta-package by using the following command:

```
$ sudo apt install ssh
```

Additional Information:

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4 :: SC-8
- NIST SP 800-53 Revision 5 :: SC-8





CCI-002420 Maintain the confidentiality and/or integrity of information during preparation for transmission.

- NIST SP 800-53 Revision 4 :: SC-8 (2)
- NIST SP 800-53 Revision 5 :: SC-8 (2)

CCI-002422 Maintain the confidentiality and/or integrity of information during reception.

- NIST SP 800-53 Revision 4 :: SC-8 (2)
- NIST SP 800-53 Revision 5 :: SC-8 (2)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

1.56 UBTU-22-255015 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

The operating system must use SSH to protect the confidentiality and integrity of transmitted information.

GROUP ID: V-260524 RULE ID: SV-260524r958908

Rationale:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

Audit:

Verify the "ssh.service" is enabled and active by using the following commands:

<pre>\$ sudo systemctl is-enabled ssh enabled \$ sudo systemctl is-active ssh active</pre>
--

If "ssh.service" is not enabled and active, this is a finding.

Remediation:

Enable and start the "ssh.service" by using the following command:

```
$ sudo systemctl enable ssh.service --now
```

Additional Information:

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4 :: SC-8
- NIST SP 800-53 Revision 5 :: SC-8





CCI-002420 Maintain the confidentiality and/or integrity of information during preparation for transmission.

- NIST SP 800-53 Revision 4 :: SC-8 (2)
- NIST SP 800-53 Revision 5 :: SC-8 (2)

CCI-002422 Maintain the confidentiality and/or integrity of information during reception.

- NIST SP 800-53 Revision 4 :: SC-8 (2)
- NIST SP 800-53 Revision 5 :: SC-8 (2)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

1.57 UBTU-22-255020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must display the Standard Mandatory DOD Notice and Consent Banner before granting any local or remote connection to the system.

GROUP ID: V-260525 RULE ID: SV-260525r958390

Rationale:

Display of a standardized and approved use notification before granting access to the publicly accessible operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DOD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

"I've read (literal ampersand) consent to terms in IS user agreem't."

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000228-GPOS-00088

Audit:

Verify the operating system displays the Standard Mandatory DOD Notice and Consent Banner before granting access to the operating system via an SSH login by using the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |  
tr '\n' ' ' | xargs sudo grep -iH 'banner'  
  
/etc/ssh/sshd_config:Banner /etc/issue.net
```

The command will return the banner option along with the name of the file that contains the SSH banner. If the line is commented out, missing, or conflicting results are returned, this is a finding.

Verify the specified banner file matches the Standard Mandatory DOD Notice and Consent Banner exactly:

```
$ cat /etc/issue.net  
  
You are accessing a U.S. Government (USG) Information System (IS) that is  
provided for USG-authorized use only. By using this IS (which includes any  
device attached to this IS), you consent to the following conditions:  
  
-The USG routinely intercepts and monitors communications on this IS for  
purposes including, but not limited to, penetration testing, COMSEC  
monitoring, network operations and defense, personnel misconduct (PM), law  
enforcement  
(LE), and counterintelligence (CI) investigations.  
  
-At any time, the USG may inspect and seize data stored on this IS.  
  
-Communications using, or data stored on, this IS are not private, are  
subject to routine monitoring, interception, and search, and may be disclosed  
or used for any USG-authorized purpose.  
  
-This IS includes security measures (e.g., authentication and access  
controls) to protect USG interests--not for your personal benefit or privacy.  
  
-Notwithstanding the above, using this IS does not constitute consent to PM,  
LE or CI investigative searching or monitoring of the content of privileged  
communications, or work product, related to personal representation or  
services by attorneys, psychotherapists, or clergy, and their assistants.  
Such communications and work product are private and confidential. See User  
Agreement for details.
```

If the banner text does not match the Standard Mandatory DOD Notice and Consent Banner exactly, this is a finding.

Remediation:

Set the parameter Banner in "/etc/ssh/sshd_config" to point to the "/etc/issue.net" file:

```
$ sudo sed -i '/^Banner/d' /etc/ssh/sshd_config  
$ sudo sed -i '$aBanner /etc/issue.net' /etc/ssh/sshd_config
```

Replace the text in "/etc/issue.net" with the Standard Mandatory DOD Notice and Consent Banner:

```
You are accessing a U.S. Government (USG) Information System (IS) that is  
provided for USG-authorized use only. By using this IS (which includes any  
device attached to this IS), you consent to the following conditions:  
  
-The USG routinely intercepts and monitors communications on this IS for  
purposes including, but not limited to, penetration testing, COMSEC  
monitoring, network operations and defense, personnel misconduct (PM), law  
enforcement (LE), and counterintelligence (CI) investigations.  
-At any time, the USG may inspect and seize data stored on this IS.  
-Communications using, or data stored on, this IS are not private, are  
subject to routine monitoring, interception, and search, and may be disclosed  
or used for any USG-authorized purpose.  
-This IS includes security measures (e.g., authentication and access  
controls) to protect USG interests--not for your personal benefit or privacy.  
-Notwithstanding the above, using this IS does not constitute consent to PM,  
LE or CI investigative searching or monitoring of the content of privileged  
communications, or work product, related to personal representation or  
services by attorneys, psychotherapists, or clergy, and their assistants.  
Such communications and work product are private and confidential. See User  
Agreement for details.
```

Restart the SSH daemon for the changes to take effect and then signal the SSH server to reload the configuration file:

```
$ sudo systemctl -s SIGHUP kill sshd
```

Additional Information:

CCI-000048 Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53 :: AC-8 a
- NIST SP 800-53 Revision 4 :: AC-8 a
- NIST SP 800-53 Revision 5 :: AC-8 a
- NIST SP 800-53A :: AC-8.1 (ii)

CCI-001384 For publicly accessible systems, display system use information with organization-defined conditions before granting further access to the publicly accessible system.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 1
- NIST SP 800-53 Revision 5 :: AC-8 c 1
- NIST SP 800-53A :: AC-8.2 (i)

CCI-001385 For publicly accessible systems, displays references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 2
- NIST SP 800-53 Revision 5 :: AC-8 c 2
- NIST SP 800-53A :: AC-8.2 (ii)

CCI-001386 For publicly accessible systems, displays references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 2
- NIST SP 800-53 Revision 5 :: AC-8 c 2
- NIST SP 800-53A :: AC-8.2 (ii)







CCI-001387 For publicly accessible systems, displays references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 2
- NIST SP 800-53 Revision 5 :: AC-8 c 2
- NIST SP 800-53A :: AC-8.2 (ii)

CCI-001388 For publicly accessible systems, includes a description of the authorized uses of the system.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 3
- NIST SP 800-53 Revision 5 :: AC-8 c 3
- NIST SP 800-53A :: AC-8.2 (iii)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.58 UBTU-22-255025 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

The operating system must not allow unattended or automatic login via SSH.

```
GROUP ID: V-260526
RULE ID: SV-260526r991591
```

Rationale:

Failure to restrict system access to authenticated users negatively impacts the operating system security.

Audit:

Verify that unattended or automatic login via SSH is disabled by using the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iEH '(permit(.*?)(passwords|environment))'

/etc/ssh/sshd_config:PermitEmptyPasswords no
/etc/ssh/sshd_config:PermitUserEnvironment no
```

If "PermitEmptyPasswords" and "PermitUserEnvironment" are not set to "no", are commented out, are missing, or conflicting results are returned, this is a finding.

Remediation:

Configure the SSH server to not allow unattended or automatic login to the system. Add or modify the following lines in the "/etc/ssh/sshd_config" file:

```
PermitEmptyPasswords no
PermitUserEnvironment no
```

Restart the SSH daemon for the changes to take effect:

```
$ sudo systemctl restart sshd.service
```

References:






1. CIS Recommendations "Ensure sshd PermitEmptyPasswords is disabled and Ensure sshd PermitUserEnvironment is disabled"

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

1.59 UBTU-22-255030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must be configured so that all network connections associated with SSH traffic terminate after becoming unresponsive.

```
GROUP ID: V-260527
RULE ID: SV-260527r986275
```

Rationale:

Terminating an unresponsive SSH session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle SSH session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, deallocating associated TCP/IP address/port pairs at the operating system level and deallocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean the operating system terminates all sessions or network access; it only ends the unresponsive session and releases the resources associated with that session.

Audit:

Verify the SSH server automatically terminates a user session after the SSH client has become unresponsive by using the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH 'clientalivecountmax'

/etc/ssh/sshd_config:ClientAliveCountMax 1
```

If "ClientAliveCountMax" is not to "1", if conflicting results are returned, is commented out, or is missing, this is a finding.

Remediation:

Configure the SSH server to terminate a user session automatically after the SSH client has become unresponsive.

Note: This setting must be applied in conjunction with UBTU-22-255040 to function correctly.

Add or modify the following line in the "/etc/ssh/sshd_config" file:

```
ClientAliveCountMax 1
```

Restart the SSH daemon for the changes to take effect:

```
$ sudo systemctl restart sshd.service
```

References:

1. CIS Recommendation "Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured"

Additional Information:

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53 :: SC-10
- NIST SP 800-53 Revision 4 :: SC-10
- NIST SP 800-53 Revision 5 :: SC-10
- NIST SP 800-53A :: SC-10.1 (ii)

1.60 UBTU-22-255035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must be configured so that all network connections associated with SSH traffic are terminated after 10 minutes of becoming unresponsive.

GROUP ID: V-260528 RULE ID: SV-260528r970703

Rationale:

Terminating an unresponsive SSH session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle SSH session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, deallocating associated TCP/IP address/port pairs at the operating system level and deallocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the unresponsive session and releases the resources associated with that session.

Audit:

Verify the SSH server automatically terminates a user session after the SSH client has been unresponsive for 10 minutes by using the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |  
tr '\n' ' ' | xargs sudo grep -iH 'ClientAliveInterval'  
  
/etc/ssh/sshd_config:ClientAliveInterval 600
```

If "ClientAliveInterval" does not exist, is not set to a value of "600" or less, if conflicting results are returned, is commented out, or is missing, this is a finding.

Remediation:

Configure the SSH server to terminate a user session automatically after the SSH client has been unresponsive for 10 minutes.

Note: This setting must be applied in conjunction with UBTU-22-255040 to function correctly.

Add or modify the following line in the "/etc/ssh/sshd_config" file:

```
ClientAliveInterval 600
```

Restart the SSH daemon for the changes to take effect:

```
$ sudo systemctl restart sshd.service
```

References:

1. CIS Recommendation "Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured"

Additional Information:

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53 :: SC-10
- NIST SP 800-53 Revision 4 :: SC-10
- NIST SP 800-53 Revision 5 :: SC-10
- NIST SP 800-53A :: SC-10.1 (ii)

1.61 UBTU-22-255040 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

The operating system must be configured so that remote X connections are disabled, unless to fulfill documented and validated mission requirements.

GROUP ID: V-260529 RULE ID: SV-260529r991589

Rationale:

The security risk of using X11 forwarding is that the client's X11 display server may be exposed to attack when the SSH client requests forwarding. A system administrator may have a stance in which they want to protect clients that may expose themselves to attack by unwittingly requesting X11 forwarding, which can warrant a "no" setting.

X11 forwarding should be enabled with caution. Users with the ability to bypass file permissions on the remote host (for the user's X11 authorization database) can access the local X11 display through the forwarded connection. An attacker may then be able to perform activities such as keystroke monitoring if the ForwardX11Trusted option is also enabled.

If X11 services are not required for the system's intended function, they should be disabled or restricted as appropriate to the system's needs.

Audit:

Verify that X11 forwarding is disabled by using the following command:

<pre>\$ sudo /usr/sbin/sshd -dd 2>&1 awk '/filename/ {print \$4}' tr -d '\r' tr '\n' ' ' xargs sudo grep -iH 'x11forwarding' /etc/ssh/sshd_config:X11Forwarding no</pre>
--

If "X11Forwarding" is set to "yes" and is not documented with the information system security officer (ISSO) as an operational requirement, is commented out, is missing, or conflicting results are returned, this is a finding.

Remediation:

Configure the SSH server to disable X11 forwarding.
Add or modify the following line in the "/etc/ssh/sshd_config" file:

```
X11Forwarding no
```

Restart the SSH daemon for the changes to take effect:

```
$ sudo systemctl restart sshd.service
```

References:

1. CIS Recommendation "Ensure sshd DisableForwarding is enabled"

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

1.62 UBTU-22-255045 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system SSH daemon must prevent remote hosts from connecting to the proxy display.

```
GROUP ID: V-260530
RULE ID: SV-260530r991589
```

Rationale:

When X11 forwarding is enabled, there may be additional exposure to the server and client displays if the sshd proxy display is configured to listen on the wildcard address. By default, sshd binds the forwarding server to the loopback address and sets the hostname part of the DISPLAY environment variable to localhost. This prevents remote hosts from connecting to the proxy display.

Audit:

Verify the SSH server prevents remote hosts from connecting to the proxy display by using the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH 'x11uselocalhost'

/etc/ssh/sshd_config:X11UseLocalhost yes
```

If "X11UseLocalhost" is set to "no", is commented out, is missing, or conflicting results are returned, this is a finding.

Remediation:

Configure the SSH server to prevent remote hosts from connecting to the proxy display. Add or modify the following line in the "/etc/ssh/sshd_config" file:

```
X11UseLocalhost yes
```

Restart the SSH daemon for the changes to take effect:





```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

1.63 UBTU-22-255050 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must configure the SSH daemon to use FIPS 140-3-approved ciphers to prevent the unauthorized disclosure of information and/or detect changes to information during transmission.

GROUP ID: V-260531 RULE ID: SV-260531r958408

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the internet) or an internal network.

Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection.

Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes.

By specifying a cipher list with the order of ciphers being in a "strongest to weakest" orientation, the system will automatically attempt to use the strongest cipher for securing SSH connections.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000394-GPOS-00174, SRG-OS-000424-GPOS-00188

Audit:

Verify the SSH server is configured to only implement FIPS-approved ciphers with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |  
tr '\n' ' ' | xargs sudo grep -iH 'ciphers'  
  
/etc/ssh/sshd_config:Ciphers aes256-ctr,aes256-gcm@openssh.com,aes192-  
ctr,aes128-ctr,aes128-gcm@openssh.com
```

If "Ciphers" does not contain only the ciphers "aes256-ctr,[aes256-gcm@openssh.com](#),aes192-ctr,aes128-ctr,[aes128-gcm@openssh.com](#)" in exact order, is commented out, is missing, or conflicting results are returned, this is a finding.

Remediation:

Configure the SSH server to only implement FIPS-approved ciphers.
Add or modify the following line in the "/etc/ssh/sshd_config" file:

```
Ciphers aes256-ctr,aes256-gcm@openssh.com,aes192-ctr,aes128-ctr,aes128-  
gcm@openssh.com
```

Restart the SSH server for the changes to take effect:

```
$ sudo systemctl restart sshd.service
```

References:

1. CIS Recommendation "Ensure sshd Ciphers are configured"

Additional Information:

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53 :: AC-17 (2)
- NIST SP 800-53 Revision 4 :: AC-17 (2)
- NIST SP 800-53 Revision 5 :: AC-17 (2)
- NIST SP 800-53A :: AC-17 (2).1







CCI-002421 Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4 :: SC-8 (1)
- NIST SP 800-53 Revision 5 :: SC-8 (1)

CCI-003123 Implement organization-defined cryptographic mechanisms to protect the confidentiality of nonlocal maintenance and diagnostic communications.

- NIST SP 800-53 Revision 4 :: MA-4 (6)
- NIST SP 800-53 Revision 5 :: MA-4 (6)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			
v7	16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.			

1.64 UBTU-22-255055 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must configure the SSH daemon to use Message Authentication Codes (MACs) employing FIPS 140-3-approved cryptographic hashes to prevent the unauthorized disclosure of information and/or detect changes to information during transmission.

GROUP ID: V-260532 RULE ID: SV-260532r991554

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless. Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the internet) or an internal network.

Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection.

Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions, which have common application in digital signatures, checksums, and message authentication codes.

Satisfies: SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173, SRG-OS-000424-GPOS-00188

Audit:

Verify the SSH server is configured to only use MACs that employ FIPS 140-3 approved ciphers by using the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |  
tr '\n' ' ' | xargs sudo grep -iH 'macs'  
  
/etc/ssh/sshd_config:MACs hmac-sha2-512,hmac-sha2-512-etm@openssh.com,hmac-  
sha2-256,hmac-sha2-256-etm@openssh.com
```

If "MACs" does not contain only the hashes "hmac-sha2-512,[hmac-sha2-512-etm@openssh.com](#),hmac-sha2-256,[hmac-sha2-256-etm@openssh.com](#)" in exact order, is commented out, is missing, or conflicting results are returned, this is a finding.

Remediation:

Configure the SSH server to only use MACs that employ FIPS 140-3 approved hashes. Add or modify the following line in the "/etc/ssh/sshd_config" file:

```
MACs hmac-sha2-512,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-256-  
etm@openssh.com
```

Restart the SSH server for the changes to take effect:

```
$ sudo systemctl reload sshd.service
```

References:

1. CIS Recommendation "Ensure sshd MACs are configured"

Additional Information:

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53 :: AC-17 (2)
- NIST SP 800-53 Revision 4 :: AC-17 (2)
- NIST SP 800-53 Revision 5 :: AC-17 (2)
- NIST SP 800-53A :: AC-17 (2).1







CCI-002421 Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4 :: SC-8 (1)
- NIST SP 800-53 Revision 5 :: SC-8 (1)

CCI-002890 Implement organization-defined cryptographic mechanisms to protect the integrity of nonlocal maintenance and diagnostic communications.

- NIST SP 800-53 Revision 4 :: MA-4 (6)
- NIST SP 800-53 Revision 5 :: MA-4 (6)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			
v7	16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.			

1.65 UBTU-22-255060 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system SSH server must be configured to use only FIPS-validated key exchange algorithms.

GROUP ID: V-260533
RULE ID: SV-260533r958408

Rationale:

Without cryptographic integrity protections provided by FIPS-validated cryptographic algorithms, information can be viewed and altered by unauthorized users without detection.

The system will attempt to use the first algorithm presented by the client that matches the server list. Listing the values "strongest to weakest" is a method to ensure the use of the strongest algorithm available to secure the SSH connection.

Audit:

Verify that the SSH server is configured to use only FIPS-validated key exchange algorithms by using the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |  
tr '\n' ' ' | xargs sudo grep -iH 'kexalgorithms'  
  
/etc/ssh/sshd_config:KexAlgorithms ecdh-sha2-nistp256,ecdh-sha2-  
nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256
```

If "KexAlgorithms" does not contain only the algorithms "ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256" in exact order, is commented out, is missing, or conflicting results are returned, this is a finding.

Remediation:

Configure the SSH server to use only FIPS-validated key exchange algorithms. Add or modify the following line in the "/etc/ssh/sshd_config" file:

```
KexAlgorithms ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256
```

Restart the SSH server for changes to take effect:

```
$ sudo systemctl restart sshd.service
```

References:





1. CIS Recommendation "Ensure sshd KexAlgorithms is configured"

Additional Information:

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53 :: AC-17 (2)
- NIST SP 800-53 Revision 4 :: AC-17 (2)
- NIST SP 800-53 Revision 5 :: AC-17 (2)
- NIST SP 800-53A :: AC-17 (2).1

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

1.66 UBTU-22-255065 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must use strong authenticators in establishing nonlocal maintenance and diagnostic sessions.

```
GROUP ID: V-260534
RULE ID: SV-260534r958510
```

Rationale:

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric.

Audit:

Verify the operating system is configured to use strong authenticators in the establishment of nonlocal maintenance and diagnostic maintenance by using the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH 'usepam'

/etc/ssh/sshd_config:UsePAM yes
```

If "UsePAM" is not set to "yes", is commented out, is missing, or conflicting results are returned, this is a finding.

Remediation:

Configure the operating system to use strong authentication when establishing nonlocal maintenance and diagnostic sessions.

Add or modify the following line to /etc/ssh/sshd_config:

```
UsePAM yes
```

Restart the SSH server for changes to take effect:

```
$ sudo systemctl restart sshd.service
```

References:






1. CIS Recommendation "Ensure sshd UsePAM is enabled"

Additional Information:

CCI-000877 Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 :: MA-4 c
- NIST SP 800-53 Revision 4 :: MA-4 c
- NIST SP 800-53 Revision 5 :: MA-4 c
- NIST SP 800-53A :: MA-4.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

1.67 UBTU-22-271010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must enable the graphical user logon banner to display the Standard Mandatory DOD Notice and Consent Banner before granting local access to the system via a graphical user logon.

GROUP ID: V-260535 RULE ID: SV-260535r958390

Rationale:

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DOD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

"I've read (literal ampersand) consent to terms in IS user agreem't."

Audit:

Verify the operating system is configured to display the Standard Mandatory DOD Notice and Consent Banner before granting access to the operating system via a graphical user logon by using the following command:

Note: If no graphical user interface is installed, this requirement is not applicable.

```
$ grep -i banner-message-enable /etc/gdm3/greeter.dconf-defaults  
  
banner-message-enable=true
```

If the value for "banner-message-enable" is set to "false", the line is commented out, or no value is returned, this is a finding.

Remediation:

Configure the operating system to display the Standard Mandatory DOD Notice and Consent Banner before granting access to the operating system via a graphical user logon.

Add or modify the following line in the "/etc/gdm3/greeter.dconf-defaults" file:

```
[org/gnome/login-screen]  
banner-message-enable=true
```

Update GDM with the new configuration by using the following commands:







```
$ sudo dconf update  
$ sudo systemctl restart gdm3
```

Additional Information:

CCI-000048 Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53 :: AC-8 a
- NIST SP 800-53 Revision 4 :: AC-8 a
- NIST SP 800-53 Revision 5 :: AC-8 a
- NIST SP 800-53A :: AC-8.1 (ii)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.68 UBTU-22-271015 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must display the Standard Mandatory DOD Notice and Consent Banner before granting local access to the system via a graphical user logon.

GROUP ID: V-260536 RULE ID: SV-260536r958390

Rationale:

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DOD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

"I've read (literal ampersand) consent to terms in IS user agreem't."

Audit:

Verify the operating system displays the Standard Mandatory DOD Notice and Consent Banner before granting access to the operating system via a graphical user logon with the command:

Note: If no graphical user interface is installed, this requirement is not applicable.

```
$ grep -i banner-message-text /etc/gdm3/greeter.dconf-defaults

banner-message-text="You are accessing a U.S. Government (USG) Information
System (IS) that is provided for USG-authorized use only.\n\nBy using this IS
(which includes any device attached to this IS), you consent to the following
conditions:\n\n-The USG routinely intercepts and monitors communications on
this IS for purposes including, but not limited to, penetration testing,
COMSEC monitoring, network operations and defense, personnel misconduct (PM),
law enforcement (LE), and counterintelligence (CI) investigations.\n\n-At any
time, the USG may inspect and seize data stored on this IS.\n\n-
Communications using, or data stored on, this IS are not private, are subject
to routine monitoring, interception, and search, and may be disclosed or used
for any USG-authorized purpose.\n\n-This IS includes security measures (e.g.,
authentication and access controls) to protect USG interests--not for your
personal benefit or privacy.\n\n-Notwithstanding the above, using this IS
does not constitute consent to PM, LE or CI investigative searching or
monitoring of the content of privileged communications, or work product,
related to personal representation or services by attorneys,
psychotherapists, or clergy, and their assistants. Such communications and
work product are private and confidential. See User Agreement for details."
```

If the banner-message-text is missing, commented out, or does not match the Standard Mandatory DOD Notice and Consent Banner exactly, this is a finding.

Remediation:

Edit the `/etc/gdm3/greeter.dconf-defaults` file.

Set the `"banner-message-text"` line to contain the appropriate banner message text as shown below:

```
banner-message-text="You are accessing a U.S. Government (USG) Information
System (IS) that is provided for USG-authorized use only.\n\nBy using this IS
(which includes any device attached to this IS), you consent to the following
conditions:\n\n-The USG routinely intercepts and monitors communications on
this IS for purposes including, but not limited to, penetration testing,
COMSEC monitoring, network operations and defense, personnel misconduct (PM),
law enforcement (LE), and counterintelligence (CI) investigations.\n\n-At any
time, the USG may inspect and seize data stored on this IS.\n\n-
Communications using, or data stored on, this IS are not private, are subject
to routine monitoring, interception, and search, and may be disclosed or used
for any USG-authorized purpose.\n\n-This IS includes security measures (e.g.,
authentication and access controls) to protect USG interests--not for your
personal benefit or privacy.\n\n-Notwithstanding the above, using this IS
does not constitute consent to PM, LE or CI investigative searching or
monitoring of the content of privileged communications, or work product,
related to personal representation or services by attorneys,
psychotherapists, or clergy, and their assistants. Such communications and
work product are private and confidential. See User Agreement for details."
```

Update GDM with the new configuration by using the following commands:







```
$ sudo dconf update
$ sudo systemctl restart gdm3
```

Additional Information:

CCI-000048 Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53 :: AC-8 a
- NIST SP 800-53 Revision 4 :: AC-8 a
- NIST SP 800-53 Revision 5 :: AC-8 a
- NIST SP 800-53A :: AC-8.1 (ii)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.69 UBTU-22-271020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must retain a user's session lock until that user reestablishes access using established identification and authentication procedures.

```
GROUP ID: V-260537
RULE ID: SV-260537r1069101
```

Rationale:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined.

Regardless of where the session lock is determined and implemented, once invoked, a session lock of the operating system must remain in place until the user reauthenticates. No other activity aside from reauthentication must unlock the system.

Audit:

Verify the operating system has a graphical user interface session lock enabled by using the following command:

Note: If no graphical user interface is installed, this requirement is not applicable.

```
$ sudo gsettings get org.gnome.desktop.screensaver lock-enabled
true
```

If "lock-enabled" is not set to "true", is commented out, or is missing, this is a finding.

Remediation:

Configure the operating system to allow a user to lock the current graphical user interface session.

Create or edit a file named /etc/dconf/db/local.d/00-screensaver with the following contents:







```
[org/gnome/desktop/screensaver]
lock-enabled=true
```

Additional Information:

CCI-000056 Retain the device lock until the user reestablishes access using established identification and authentication procedures.

- NIST SP 800-53 :: AC-11 b
- NIST SP 800-53 Revision 4 :: AC-11 b
- NIST SP 800-53 Revision 5 :: AC-11 b
- NIST SP 800-53A :: AC-11.1 (iii)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			

1.70 UBTU-22-271025 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must initiate a graphical session lock after 15 minutes of inactivity.

GROUP ID: V-260538 RULE ID: SV-260538r1069119
--

Rationale:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined.

Regardless of where the session lock is determined and implemented, once invoked, a session lock of the operating system must remain in place until the user reauthenticates. No other activity aside from reauthentication must unlock the system.

Audit:

Verify the operating system has a graphical user interface session lock configured to activate after 15 minutes of inactivity by using the following commands:

Note: If no graphical user interface is installed, this requirement is not applicable.

Get the following settings to verify the graphical user interface session is configured to lock the graphical user session after 15 minutes of inactivity:

```
$ gsettings get org.gnome.desktop.screensaver lock-enabled
true

$ gsettings get org.gnome.desktop.screensaver lock-delay
uint32 0

$ gsettings get org.gnome.desktop.session idle-delay
int32 900
```

If "lock-enabled" is not set to "true", is commented out, or is missing, this is a finding.

If "lock-delay" is set to a value greater than "0", or if "idle-delay" is set to a value greater than "900", is commented out, or is missing, this is a finding.

Remediation:

Configure the operating system to lock the current graphical user interface session after 15 minutes of inactivity.

Create or edit a file named /etc/dconf/db/local.d/00-screensaver with the following contents:

```
[org/gnome/desktop/screensaver]
lock-enabled=true
lock-delay=0

[org/gnome/desktop/session]
idle-delay=600
```

References:







1. CIS Recommendation "Ensure GDM screen locks when the user is idle"

Additional Information:

CCI-000057 The information system initiates a session lock after the organization-defined time period of inactivity.

- NIST SP 800-53 :: AC-11 a
- NIST SP 800-53 Revision 4 :: AC-11 a
- NIST SP 800-53 Revision 5 :: AC-11 a
- NIST SP 800-53A :: AC-11.1 (ii)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.71 UBTU-22-271030 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

The operating system must disable the x86 Ctrl-Alt-Delete key sequence if a graphical user interface is installed.

```
GROUP ID: V-260539
RULE ID: SV-260539r1069103
```

Rationale:

A locally logged-on user who presses Ctrl-Alt-Delete, when at the console, can reboot the system. If accidentally pressed, as could happen in the case of a mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot. In the graphical environment, risk of unintentional reboot from the Ctrl-Alt-Delete sequence is reduced because the user will be prompted before any action is taken.

Audit:

Verify the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed when using a graphical user interface by using the following command:

Note: If no graphical user interface is installed, this requirement is not applicable.

```
$ gsettings get org.gnome.settings-daemon.plugins.media-keys logout
@as []
```

If the "logout" key is bound to an action, is commented out, or is missing, this is a finding.

Remediation:

Configure the operating system to disable the Ctrl-Alt-Delete sequence when using a graphical user interface.

Create or edit a file named /etc/dconf/db/local.d/00-screensaver with the following contents:

```
[org/gnome/settings-daemon/plugins/media-keys]
logout=""
```

Update the dconf settings:







```
$ sudo dconf update
```


Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.72 UBTU-22-291010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must disable automatic mounting of Universal Serial Bus (USB) mass storage driver.

```
GROUP ID: V-260540
RULE ID: SV-260540r986276
```

Rationale:

Without authenticating devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity.

Peripherals include, but are not limited to, such devices as flash drives, external storage, and printers.

Audit:

Verify the operating system disables ability to load the USB storage kernel module by using the following command:

```
$ grep usb-storage /etc/modprobe.d/* | grep "/bin/false"

/etc/modprobe.d/stig.conf:install usb-storage /bin/false
```

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

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

```
$ grep usb-storage /etc/modprobe.d/* | grep -i "blacklist"

/etc/modprobe.d/stig.conf:blacklist usb-storage
```

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

Remediation:

Configure the operating system to disable using the USB storage kernel module.
Create and/or append a custom file under "/etc/modprobe.d/" to contain the following:

```
$ sudo su -c "echo install usb-storage /bin/false >> /etc/modprobe.d/stig.conf"
```

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

```
$ sudo su -c "echo blacklist usb-storage >> /etc/modprobe.d/stig.conf"
```

References:

1. CIS Recommendation "Ensure usb-storage kernel module is not available"

Additional Information:






CCI-001958 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 Revision 4 :: IA-3
- NIST SP 800-53 Revision 5 :: IA-3

CCI-003959 Prohibit the use or connection of unauthorized hardware components.

- NIST SP 800-53 Revision 5 :: CM-7 (9) (b)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.3 <u>Disable Autorun and Autoplay for Removable Media</u> Disable autorun and autoplay auto-execute functionality for removable media.			
v7	13.7 <u>Manage USB Devices</u> If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.			

1.73 UBTU-22-291015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must disable all wireless network adapters.

GROUP ID: V-260541
RULE ID: SV-260541r958358

Rationale:

Without protection of communications with wireless peripherals, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read, altered, or used to compromise the operating system.

This requirement applies to wireless peripheral technologies (e.g., wireless mice, keyboards, displays, etc.) used with an operating system. Wireless peripherals (e.g., Wi-Fi/Bluetooth/IR Keyboards, Mice, and Pointing Devices and Near Field Communications [NFC]) present a unique challenge by creating an open, unsecured port on a computer. Wireless peripherals must meet DOD requirements for wireless data transmission and be approved for use by the AO. Even though some wireless peripherals, such as mice and pointing devices, do not ordinarily carry information that need to be protected, modification of communications with these wireless peripherals may be used to compromise the operating system. Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of communications with wireless peripherals can be accomplished by physical means (e.g., employing physical barriers to wireless radio frequencies) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa. If the wireless peripheral is only passing telemetry data, encryption of the data may not be required.

Audit:

Verify that there are no wireless interfaces configured on the system by using the following command:

Note: If the system does not have any physical wireless network radios, this requirement is not applicable.

```
$ cat /proc/net/wireless
```

If any wireless interface names are listed under "Interface" and have not been documented and approved by the information system security officer (ISSO), this is a finding.

Remediation:

Disable all wireless network interfaces by using the following command:

```
$ sudo ifdown <wireless_interface_name>
```

For each interface listed, find their respective module by using the following command:

```
$ basename $(readlink -f  
/sys/class/net/<wireless_interface_name>/device/driver
```

where <wireless_interface_name> must be substituted by the actual interface name. Create and/or append a custom file under "/etc/modprobe.d/" by using the following command:

```
$ sudo su -c "echo install <module_name> /bin/false >>  
/etc/modprobe.d/stig.conf"
```

where <module_name> must be substituted by the actual module name. For each module from the system, execute the following command to remove it:

```
$ sudo modprobe -r <module_name>
```

References:

1. CIS Recommendation "Ensure wireless interfaces are disabled"

Additional Information:

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4 :: SC-8
- NIST SP 800-53 Revision 5 :: SC-8

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	15.4 <u>Disable Wireless Access on Devices if Not Required</u> Disable wireless access on devices that do not have a business purpose for wireless access.			●
v7	15.5 <u>Limit Wireless Access on Client Devices</u> Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.			●

1.74 UBTU-22-411010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must prevent direct login into the root account.

```
GROUP ID: V-260542
RULE ID: SV-260542r1015006
```

Rationale:

To ensure individual accountability and prevent unauthorized access, organizational users must be individually identified and authenticated.

A group authenticator is a generic account used by multiple individuals. Use of a group authenticator alone does not uniquely identify individual users. Examples of the group authenticator is the Unix OS "root" user account, the Windows "Administrator" account, the "sa" account, or a "helpdesk" account.

For example, the Unix and Windows operating systems offer a "switch user" capability allowing users to authenticate with their individual credentials and, when needed, "switch" to the administrator role. This method provides for unique individual authentication prior to using a group authenticator.

Users (and any processes acting on behalf of users) must be uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization, which outlines specific user actions that can be performed on the operating system without identification or authentication.

Requiring individuals to be authenticated with an individual authenticator prior to using a group authenticator allows for traceability of actions, as well as adding an additional level of protection of the actions that can be taken with group account knowledge.

Audit:

Verify the operating system prevents direct logins to the root account by using the following command:

```
$ sudo passwd -S root
root L 08/09/2022 0 99999 7 -1
```

If the output does not contain "L" in the second field to indicate the account is locked, this is a finding.

Remediation:

Configure the operating system to prevent direct logins to the root account by using the following command:

```
$ sudo passwd -l root
```

References:

1. CIS Recommendation "Ensure root account is locked"

Additional Information:







CCI-004045 Require users to be individually authenticated before granting access to the shared accounts or resources.

- NIST SP 800-53 Revision 5 :: IA-2 (5)

CCI-000770 The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

- NIST SP 800-53 :: IA-2 (5) (b)
- NIST SP 800-53 Revision 4 :: IA-2 (5)
- NIST SP 800-53A :: IA-2 (5).2 (ii)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.75 UBTU-22-411015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must uniquely identify interactive users.

```
GROUP ID: V-260543  
RULE ID: SV-260543r958482
```

Rationale:

To ensure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1. Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and
2. Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Satisfies: SRG-OS-000104-GPOS-00051, SRG-OS-000121-GPOS-00062

Audit:

Verify the operating system contains no duplicate User IDs (UIDs) for interactive users by using the following command:

```
$ awk -F ":" 'list[$3]++{print $1, $3}' /etc/passwd
```

If output is produced and the accounts listed are interactive user accounts, this is a finding.

Remediation:

Edit the file "/etc/passwd" and provide each interactive user account that has a duplicate UID with a unique UID.

References:

1. CIS Recommendation "Ensure root account is locked"

Additional Information:

CCI-000764 Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53 :: IA-2
- NIST SP 800-53 Revision 4 :: IA-2
- NIST SP 800-53 Revision 5 :: IA-2
- NIST SP 800-53A :: IA-2.1

CCI-000804 Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

- NIST SP 800-53 :: IA-8
- NIST SP 800-53 Revision 4 :: IA-8
- NIST SP 800-53 Revision 5 :: IA-8
- NIST SP 800-53A :: IA-8.1

1.76 UBTU-22-411025 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must enforce 24 hours/one day as the minimum password lifetime. Passwords for new users must have a 24 hours/one day minimum password lifetime restriction.

```
GROUP ID: V-260545
RULE ID: SV-260545r1015007
```

Rationale:

Enforcing a minimum password lifetime helps to prevent repeated password changes to defeat the password reuse or history enforcement requirement. If users are allowed to immediately and continually change their password, then the password could be repeatedly changed in a short period of time to defeat the organization's policy regarding password reuse.

Audit:

Verify the operating system enforces a 24 hours/one day minimum password lifetime for new user accounts by using the following command:

```
$ grep -i pass_min_days /etc/login.defs

PASS_MIN_DAYS      1
```

If "PASS_MIN_DAYS" is less than "1", is commented out, or is missing, this is a finding.

Remediation:

Configure the operating system to enforce a 24 hours/one day minimum password lifetime.

Add or modify the following line in the "/etc/login.defs" file:

```
PASS_MIN_DAYS      1
```

References:

1. CIS Recommendation "Ensure minimum password days is configured"

Additional Information:






CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-000198 The information system enforces minimum password lifetime restrictions.

- NIST SP 800-53 :: IA-5 (1) (d)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (d)
- NIST SP 800-53A :: IA-5 (1).1 (v)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

1.77 UBTU-22-411030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must enforce a 60-day maximum password lifetime restriction. Passwords for new users must have a 60-day maximum password lifetime restriction.

```
GROUP ID: V-260546
RULE ID: SV-260546r1038967
```

Rationale:

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.

Audit:

Verify the operating system enforces a 60-day maximum password lifetime for new user accounts by using the following command:

```
$ grep -i pass_max_days /etc/login.defs
PASS_MAX_DAYS      60
```

If "PASS_MAX_DAYS" is less than "60", is commented out, or is missing, this is a finding.

Remediation:

Configure the operating system to enforce a 60-day maximum password lifetime. Add or modify the following line in the "/etc/login.defs" file:

```
PASS_MAX_DAYS      60
```

References:

1. CIS Recommendation "Ensure password expiration is configured"

Additional Information:






CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-000199 The information system enforces maximum password lifetime restrictions.

- NIST SP 800-53 :: IA-5 (1) (d)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (d)
- NIST SP 800-53A :: IA-5 (1).1 (v)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 <u>Use Unique Passwords</u> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

1.78 UBTU-22-411035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must disable account identifiers (individuals, groups, roles, and devices) after 35 days of inactivity.

```
GROUP ID: V-260547  
RULE ID: SV-260547r1015009
```

Rationale:

Inactive identifiers pose a risk to systems and applications because attackers may exploit an inactive identifier and potentially obtain undetected access to the system. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained.

Operating systems need to track periods of inactivity and disable application identifiers after 35 days of inactivity.

Audit:

Verify the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity by using the following command:

Check the account inactivity value by performing the following command:

```
$ grep INACTIVE /etc/default/useradd  
  
INACTIVE=35
```

If "INACTIVE" is set to "-1" or is not set to "35", is commented out, or is missing, this is a finding.

Remediation:

Configure the operating system to disable account identifiers after 35 days of inactivity after the password expiration.

Run the following command to change the configuration for adduser:

```
$ sudo useradd -D -f 35
```

Note: DOD recommendation is 35 days, but a lower value is acceptable. The value "0" will disable the account immediately after the password expires.

References:

1. CIS Recommendation "Ensure inactive password lock is configured"

Additional Information:

CCI-003627 Disable accounts when the accounts have expired.

- NIST SP 800-53 Revision 5 :: AC-2 (3) (a)






CCI-003628 Disable accounts when the accounts are no longer associated to a user.

- NIST SP 800-53 Revision 5 :: AC-2 (3) (b)

CCI-000795 The organization manages information system identifiers by disabling the identifier after an organization-defined time period of inactivity.

- NIST SP 800-53 :: IA-4 e
- NIST SP 800-53 Revision 4 :: IA-4 e
- NIST SP 800-53A :: IA-4.1 (iii)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

1.79 UBTU-22-411040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must automatically expire temporary accounts within 72 hours.

GROUP ID: V-260548
RULE ID: SV-260548r958364

Rationale:

Temporary accounts are privileged or nonprivileged accounts established during pressing circumstances, such as new software or hardware configuration or an incident response, where the need for prompt account activation requires bypassing normal account authorization procedures. If any inactive temporary accounts are left enabled on the system and are not either manually removed or automatically expired within 72 hours, the security posture of the system will be degraded and exposed to exploitation by unauthorized users or insider threat actors.

Temporary accounts are different from emergency accounts. Emergency accounts, also known as "last resort" or "break glass" accounts, are local logon accounts enabled on the system for emergency use by authorized system administrators to manage a system when standard logon methods are failing or not available. Emergency accounts are not subject to manual removal or scheduled expiration requirements.

The automatic expiration of temporary accounts may be extended as needed by the circumstances, but it must not be extended indefinitely. A documented permanent account should be established for privileged users who need long-term maintenance accounts.

Satisfies: SRG-OS-000002-GPOS-00002, SRG-OS-000123-GPOS-00064

Audit:

Verify temporary accounts have been provisioned with an expiration date of 72 hours by using the following command:

```
$ sudo chage -l <temporary_account_name> | grep -E '(Password|Account) expires'
```

Password expires : Apr 1, 2024
Account expires : Apr 1, 2024

Verify each of these accounts has an expiration date set within 72 hours. If any temporary accounts have no expiration date set or do not expire within 72 hours, this is a finding.

Remediation:

Configure the operating system to expire temporary accounts after 72 hours by using the following command:

```
$ sudo chage -E $(date -d +3days +%Y-%m-%d) <temporary_account_name>
```

Additional Information:






CCI-000016 Automatically remove or disable temporary and emergency accounts after an organization-defined time-period for each type of account.

- NIST SP 800-53 :: AC-2 (2)
- NIST SP 800-53 Revision 4 :: AC-2 (2)
- NIST SP 800-53 Revision 5 :: AC-2 (2)
- NIST SP 800-53A :: AC-2 (2).1 (ii)

CCI-001682 Automatically removes or disables emergency accounts after an organization-defined time period for each type of account.

- NIST SP 800-53 :: AC-2 (2)
- NIST SP 800-53 Revision 4 :: AC-2 (2)
- NIST SP 800-53 Revision 5 :: AC-2 (2)
- NIST SP 800-53A :: AC-2 (2).1 (ii)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	16.10 <u>Ensure All Accounts Have An Expiration Date</u> Ensure that all accounts have an expiration date that is monitored and enforced.			

1.80 UBTU-22-411045 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts have been made.

```
GROUP ID: V-260549
RULE ID: SV-260549r958388
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-forcing, is reduced. Limits are imposed by locking the account.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Verify that the operating system utilizes the "pam_faillock" module by using the following command:

```
$ grep faillock /etc/pam.d/common-auth

auth      [default=die]    pam_faillock.so authfail
auth      sufficient     pam_faillock.so authsucc
```

If the "pam_faillock.so" module is not present in the "/etc/pam.d/common-auth" file, this is a finding.

Verify the "pam_faillock" module is configured to use the following options:

```
$ sudo grep -Ew 'silent|audit|deny|fail_interval|unlock_time'
/etc/security/faillock.conf

audit
silent
deny = 3
fail_interval = 900
unlock_time = 0
```

If "audit" is commented out, or is missing, this is a finding.

If "silent" is commented out, or is missing, this is a finding.

If "deny" is set to a value greater than "3", is commented out, or is missing, this is a finding.

If "fail_interval" is set to a value greater than "900", is commented out, or is missing, this is a finding.

If "unlock_time" is not set to "0", is commented out, or is missing, this is a finding.

Remediation:

Configure the operating system to utilize the "pam_faillock" module.
Add or modify the following lines in the "/etc/pam.d/common-auth" file, below the "auth" definition for "pam_unix.so":

```
auth [default=die] pam_faillock.so authfail
auth sufficient pam_faillock.so authsucc
```

Configure the "pam_faillock" module to use the following options.
Add or modify the following lines in the "/etc/security/faillock.conf" file:

```
audit
silent
deny = 3
fail_interval = 900
unlock_time = 0
```

References:

1. CIS Recommendation "Ensure lockout for failed password attempts is configured"

Additional Information:






CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53 :: AC-7 a
- NIST SP 800-53 Revision 4 :: AC-7 a
- NIST SP 800-53 Revision 5 :: AC-7 a
- NIST SP 800-53A :: AC-7.1 (ii)

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4 :: AC-7 b
- NIST SP 800-53 Revision 5 :: AC-7 b

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.2 <u>Establish an Access Revoking Process</u> Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v7	16.7 <u>Establish Process for Revoking Access</u> Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.			

1.81 UBTU-22-412010 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must enforce a delay of at least four seconds between logon prompts following a failed logon attempt.

```
GROUP ID: V-260550
RULE ID: SV-260550r991588
```

Rationale:

Limiting the number of logon attempts over a certain time interval reduces the chances that an unauthorized user may gain access to an account.

Audit:

Verify the operating system enforces a delay of at least four seconds between logon prompts following a failed logon attempt by using the following command:

```
$ grep pam_faildelay /etc/pam.d/common-auth

auth      required      pam_faildelay.so      delay=4000000
```

If "delay" is not set to "4000000" or greater, the line is commented out, or is missing, this is a finding.

Remediation:

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

Add or modify the following line in the "/etc/pam.d/common-auth" file:







```
auth      required      pam_faildelay.so      delay=4000000
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.82 UBTU-22-412020 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

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

```
GROUP ID: V-260552  
RULE ID: SV-260552r958398
```

Rationale:

The operating system management includes the ability to control the number of users and user sessions that utilize an operating system. Limiting the number of allowed users and sessions per user is helpful in reducing the risks related to denial-of-service (DoS) attacks.

This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based upon mission needs and the operational environment for each system.

Audit:

Verify the operating system limits the number of concurrent sessions to 10 for all accounts and/or account types by using the following command:

```
$ sudo grep -r -s '^[^#].*maxlogins' /etc/security/limits.conf  
/etc/security/limits.d/*.conf  
  
/etc/security/limits.conf:* hard maxlogins 10
```

If "maxlogins" does not have a value of "10" or less, is commented out, or is missing, this is a finding.

Remediation:

Configure the operating system to limit the number of concurrent sessions to 10 for all accounts and/or account types.

Add or modify the following line at the top of the "/etc/security/limits.conf" file:







```
* hard maxlogins 10
```

Additional Information:

CCI-000054 Limit the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number.

- NIST SP 800-53 :: AC-10
- NIST SP 800-53 Revision 4 :: AC-10
- NIST SP 800-53 Revision 5 :: AC-10
- NIST SP 800-53A :: AC-10.1 (ii)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.83 UBTU-22-412025 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must allow users to directly initiate a session lock for all connection types.

```
GROUP ID: V-260553
RULE ID: SV-260553r1015010
```

Rationale:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined. Rather than be forced to wait for a period of time to expire before the user session can be locked, the operating system need to provide users with the ability to manually invoke a session lock so users may secure their session if they need to temporarily vacate the immediate physical vicinity.

Satisfies: SRG-OS-000030-GPOS-00011, SRG-OS-000031-GPOS-00012

Audit:

Verify the operating system has the "vlock" package installed by using the following command:

```
$ dpkg -l | grep vlock
ii      vlock      2.2.2-10    amd64      Virtual Console locking program
```

If "vlock" is not installed, this is a finding.

Remediation:

Install the "vlock" package by using the following command:

```
$ sudo apt-get install vlock
```

Additional Information:

CCI-000057 The information system initiates a session lock after the organization-defined time period of inactivity.

- NIST SP 800-53 :: AC-11 a
- NIST SP 800-53 Revision 4 :: AC-11 a
- NIST SP 800-53 Revision 5 :: AC-11 a
- NIST SP 800-53A :: AC-11.1 (ii)







CCI-000060 Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

- NIST SP 800-53 :: AC-11 (1)
- NIST SP 800-53 Revision 4 :: AC-11 (1)
- NIST SP 800-53 Revision 5 :: AC-11 (1)
- NIST SP 800-53A :: AC-11 (1).1

CCI-000058 The information system provides the capability for users to directly initiate session lock mechanisms.

- NIST SP 800-53 :: AC-11 a
- NIST SP 800-53 Revision 4 :: AC-11 a
- NIST SP 800-53A :: AC-11

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.			
v7	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.			

1.84 UBTU-22-412030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must automatically exit interactive command shell user sessions after 15 minutes of inactivity.

```
GROUP ID: V-260554
RULE ID: SV-260554r958636
```

Rationale:

Terminating an idle interactive command shell user session within a short time period reduces the window of opportunity for unauthorized personnel to take control of it when left unattended in a virtual terminal or physical console.

Audit:

Verify the operating system is configured to automatically exit interactive command shell user sessions after 15 minutes of inactivity or less by using the following command:

```
$ sudo grep -E "\bTMOUT=[0-9]+" /etc/bash.bashrc /etc/profile.d/*
/etc/profile.d/99-terminal_tmout.sh:TMOUT=900
```

If "TMOUT" is not set to "900" or less, is set to "0", is commented out, or missing, this is a finding.

Remediation:

Configure the operating system to exit interactive command shell user sessions after 15 minutes of inactivity.

Create and/or append a custom file under "/etc/profile.d/" by using the following command:

```
$ sudo su -c "echo TMOUT=900 >> /etc/profile.d/99-terminal_tmout.sh"
```

This will set a timeout value of 15 minutes for all future sessions.

To set the timeout for the current sessions, execute the following command over the terminal session:

```
$ export TMOUT=900
```

References:







1. CIS Recommendation "Ensure default user shell timeout is configured"

Additional Information:

CCI-002361 Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

- NIST SP 800-53 Revision 4 :: AC-12
- NIST SP 800-53 Revision 5 :: AC-12

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.			
v7	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.			

1.85 UBTU-22-412035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system default filesystem permissions must be defined in such a way that all authenticated users can read and modify only their own files.

```
GROUP ID: V-260555  
RULE ID: SV-260555r991590
```

Rationale:

Setting the most restrictive default permissions ensures newly created accounts do not have unnecessary access.

Audit:

Verify the operating system defines default permissions for all authenticated users in such a way that the user can read and modify only their own files by using the following command:

```
$ grep -i '^s*umask' /etc/login.defs  
  
UMASK 077
```

If the "UMASK" variable is set to "000", this is a finding with the severity raised to a CAT I.

If "UMASK" is not set to "077", is commented out, or is missing, this is a finding.

Remediation:

Configure the operating system to define the default permissions for all authenticated users in such a way that the user can read and modify only their own files.

Add or modify the following line in the "/etc/login.defs" file:

```
UMASK 077
```

References:







1. CIS Recommendation "Ensure default user umask is 077 or more restrictive"

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

CIS Controls:

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

1.86 UBTU-22-431010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must have the "apparmor" package installed.

```
GROUP ID: V-260556
RULE ID: SV-260556r958702
```

Rationale:

Control of program execution is a mechanism used to prevent execution of unauthorized programs. Some operating systems may provide a capability that runs counter to the mission or provides users with functionality that exceeds mission requirements. This includes functions and services installed at the operating system level.

Some of the programs, installed by default, may be harmful or may not be necessary to support essential organizational operations (e.g., key missions, functions). Removal of executable programs is not always possible; therefore, establishing a method of preventing program execution is critical to maintaining a secure system baseline.

Methods for complying with this requirement include restricting execution of programs in certain environments, while preventing execution in other environments; or limiting execution of certain program functionality based on organization-defined criteria (e.g., privileges, subnets, sandboxed environments, or roles).

Satisfies: SRG-OS-000312-GPOS-00124, SRG-OS-000368-GPOS-00154, SRG-OS-000370-GPOS-00155

Audit:

Verify the operating system has the "apparmor" package installed by using the following command:

```
$ dpkg -l | grep apparmor

ii      apparmor      3.0.4-2ubuntu2.3      amd64      user-space parser utility
for AppArmor
```

If the "apparmor" package is not installed, this is a finding.

Remediation:

Install the "appArmor" package by using the following command:

```
$ sudo apt-get install apparmor
```

References:

1. CIS Recommendation "Ensure AppArmor is installed"

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)







CCI-001774 Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system.

- NIST SP 800-53 Revision 4 :: CM-7 (5) (b)
- NIST SP 800-53 Revision 5 :: CM-7 (5) (b)

CCI-002165 Enforce organization-defined discretionary access control policies over defined subjects and objects.

- NIST SP 800-53 Revision 4 :: AC-3 (4)
- NIST SP 800-53 Revision 5 :: AC-3 (4)

CIS Controls:

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

1.87 UBTU-22-431015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must be configured to use AppArmor.

```
GROUP ID: V-260557
RULE ID: SV-260557r958804
```

Rationale:

Control of program execution is a mechanism used to prevent execution of unauthorized programs. Some operating systems may provide a capability that runs counter to the mission or provides users with functionality that exceeds mission requirements. This includes functions and services installed at the operating system level.

Some of the programs, installed by default, may be harmful or may not be necessary to support essential organizational operations (e.g., key missions, functions). Removal of executable programs is not always possible; therefore, establishing a method of preventing program execution is critical to maintaining a secure system baseline.

Methods for complying with this requirement include restricting execution of programs in certain environments, while preventing execution in other environments; or limiting execution of certain program functionality based on organization-defined criteria (e.g., privileges, subnets, sandboxed environments, or roles).

Satisfies: SRG-OS-000368-GPOS-00154, SRG-OS-000370-GPOS-00155, SRG-OS-000324-GPOS-00125

Audit:

Verify the operating system AppArmor is active by using the following commands:

```
$ systemctl is-enabled apparmor.service
enabled
$ systemctl is-active apparmor.service
active
```

If "apparmor.service" is not enabled and active, this is a finding.

Check if AppArmor profiles are loaded and enforced by using the following command:

```
$ sudo apparmor_status | grep -i profile

32 profiles are loaded.
32 profiles are in enforce mode.
0 profiles are in complain mode.
0 profiles are in kill mode.
0 profiles are in unconfined mode.
2 processes have profiles defined.
0 processes are unconfined but have a profile defined.
```

If no profiles are loaded and enforced, this is a finding.

Remediation:

Enable and start "apparmor.service" by using the following command:

```
$ sudo systemctl enable apparmor.service --now
```

Note: AppArmor must have properly configured profiles for applications and home directories. All configurations will be based on the actual system setup and organization and normally are on a per role basis. See the AppArmor documentation for more information on configuring profiles.

References:

1. CIS Recommendations "Ensure AppArmor is installed, enabled, and active" & "Ensure all AppArmor Profiles are enforcing"

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

CCI-001774 Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system.

- NIST SP 800-53 Revision 4 :: CM-7 (5) (b)
- NIST SP 800-53 Revision 5 :: CM-7 (5) (b)

CCI-002235 Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 <u>Define and Maintain Role-Based Access Control</u> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	14.7 <u>Enforce Access Control to Data through Automated Tools</u> Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.			●

1.88 UBTU-22-432010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must require users to reauthenticate for privilege escalation or when changing roles.

```
GROUP ID: V-260558  
RULE ID: SV-260558r1050789
```

Rationale:

Without reauthentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user reauthenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157

Audit:

Verify the "/etc/sudoers" file has no occurrences of "NOPASSWD" or "!authenticate" by using the following command:

```
$ sudo grep -Ei '(nopasswd|!authenticate)' /etc/sudoers /etc/sudoers.d/*
```

If any occurrences of "NOPASSWD" or "!authenticate" return from the command, this is a finding.

Remediation:

Remove any occurrence of "NOPASSWD" or "!authenticate" found in "/etc/sudoers" file or files in the "/etc/sudoers.d" directory.

References:

1. CIS Recommendations "Ensure re-authentication for privilege escalation is not disabled globally" & "Ensure users must provide password for privilege escalation"

Additional Information:







CCI-004895 Permit users to invoke the trusted communications path for communications between the user and the organization-defined security functions, including at a minimum, authentication and re-authentication.

- NIST SP 800-53 Revision 5 :: SC-11 b

CCI-002038 The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4 :: IA-11

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			
v7	4.3 <u>Ensure the Use of Dedicated Administrative Accounts</u> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.			

1.89 UBTU-22-432015 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The operating system must ensure only users who need access to security functions are part of sudo group.

```
GROUP ID: V-260559
RULE ID: SV-260559r958518
```

Rationale:

An isolation boundary provides access control and protects the integrity of the hardware, software, and firmware that perform security functions.

Security functions are the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Operating systems implement code separation (i.e., separation of security functions from nonsecurity functions) in a number of ways, including through the provision of security kernels via processor rings or processor modes. For nonkernel code, security function isolation is often achieved through file system protections that serve to protect the code on disk and address space protections that protect executing code.

Developers and implementers can increase the assurance in security functions by employing well-defined security policy models; structured, disciplined, and rigorous hardware and software development techniques; and sound system/security engineering principles. Implementation may include isolation of memory space and libraries.

The operating system restricts access to security functions through the use of access control mechanisms and by implementing least privilege capabilities.

Audit:

Verify the sudo group has only members who require access to security functions by using the following command:

```
$ grep sudo /etc/group

sudo:x:27:<username>
```

If the sudo group contains users not needing access to security functions, this is a finding.

Remediation:

Configure the sudo group with only members requiring access to security functions.
To remove a user from the sudo group, run:







```
$ sudo gpasswd -d <username> sudo
```

Additional Information:

CCI-001084 Isolate security functions from nonsecurity functions.

- NIST SP 800-53 :: SC-3
- NIST SP 800-53 Revision 4 :: SC-3
- NIST SP 800-53 Revision 5 :: SC-3
- NIST SP 800-53A :: SC-3.1 (ii)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			
v7	<u>4.3 Ensure the Use of Dedicated Administrative Accounts</u> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.			

1.90 UBTU-22-611010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must enforce password complexity by requiring at least one uppercase character be used.

```
GROUP ID: V-260560
RULE ID: SV-260560r1015012
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

Verify the operating system enforces password complexity by requiring at least one uppercase character be used by using the following command:

```
$ grep -i ucredit /etc/security/pwquality.conf
ucredit = -1
```

If "ucredit" is greater than "-1", is commented out, or is missing, this is a finding.

Remediation:

Configure the operating system to enforce password complexity by requiring that at least one uppercase character be used.

Add or modify the following line in the "/etc/security/pwquality.conf" file:

```
ucredit = -1
```

References:

1. CIS Recommendation "Ensure password creation requirements are configured"

Additional Information:






CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-000192 The information system enforces password complexity by the minimum number of upper case characters used.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (v)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

1.91 UBTU-22-611015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must enforce password complexity by requiring at least one lowercase character be used.

```
GROUP ID: V-260561
RULE ID: SV-260561r1015013
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

Verify the operating system enforces password complexity by requiring that at least one lowercase character be used by using the following command:

```
$ grep -i lcredit /etc/security/pwquality.conf

lcredit = -1
```

If "lcredit" is greater than "-1", is commented out, or is missing, this is a finding.

Remediation:

Configure the operating system to enforce password complexity by requiring that at least one lowercase character be used.

Add or modify the following line in the "/etc/security/pwquality.conf" file:

```
lcredit = -1
```

References:

1. CIS Recommendation "Ensure password creation requirements are configured"

Additional Information:






CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-000193 The information system enforces password complexity by the minimum number of lower case characters used.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (v)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

1.92 UBTU-22-611020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must enforce password complexity by requiring that at least one numeric character be used.

```
GROUP ID: V-260562
RULE ID: SV-260562r1015014
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

Verify the operating system enforces password complexity by requiring that at least one numeric character be used by using the following command:

```
$ grep -i dcredit /etc/security/pwquality.conf

dcredit = -1
```

If "dcredit" is greater than "-1", is commented out, or is missing, this is a finding.

Remediation:

Configure the operating system to enforce password complexity by requiring that at least one numeric character be used.

Add or modify the following line in the "/etc/security/pwquality.conf" file:

```
dcredit = -1
```

References:

1. CIS Recommendation "Ensure password creation requirements are configured"

Additional Information:






CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-000194 The information system enforces password complexity by the minimum number of numeric characters used.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (v)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

1.93 UBTU-22-611025 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must enforce password complexity by requiring that at least one special character be used.

```
GROUP ID: V-260563
RULE ID: SV-260563r1015015
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity or strength is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor in determining how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Special characters are those characters that are not alphanumeric. Examples include: ~ ! @ # \$ % ^ * .

Audit:

Verify the operating system enforces password complexity by requiring that at least one special character be used by using the following command:

```
$ grep -i ocredit /etc/security/pwquality.conf
ocredit = -1
```

If "ocredit" is greater than "-1", is commented out, or is missing, this is a finding.

Remediation:

Configure the operating system to enforce password complexity by requiring that at least one special character be used.

Add or modify the following line in the "/etc/security/pwquality.conf" file:

```
ocredit = -1
```

References:

1. CIS Recommendation "Ensure password creation requirements are configured"

Additional Information:






CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-001619 The information system enforces password complexity by the minimum number of special characters used.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (v)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

1.94 UBTU-22-611030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must prevent the use of dictionary words for passwords.

```
GROUP ID: V-260564
RULE ID: SV-260564r991587
```

Rationale:

If the operating system allows the user to select passwords based on dictionary words, then this increases the chances of password compromise by increasing the opportunity for successful guesses and brute-force attacks.

Audit:

Verify the operating system prevents the use of dictionary words for passwords by using the following command:

```
$ grep -i dictcheck /etc/security/pwquality.conf

dictcheck = 1
```

If "dictcheck" is not set to "1", is commented out, or is missing, this is a finding.

Remediation:

Configure the operating system to prevent the use of dictionary words for passwords. Add or modify the following line in the "/etc/security/pwquality.conf" file:

```
dictcheck = 1
```

References:






1. CIS Recommendation "Ensure preventing the use of dictionary words for passwords is configured"

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 <u>Use Unique Passwords</u> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

1.95 UBTU-22-611035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must enforce a minimum 15-character password length.

```
GROUP ID: V-260565  
RULE ID: SV-260565r1015016
```

Rationale:

The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. Use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the

Audit:

Verify the pwquality configuration file enforces a minimum 15-character password length by using the following command:

```
$ grep -i minlen /etc/security/pwquality.conf  
  
minlen = 15
```

If "minlen" is not "15" or higher, is commented out, or is missing, this is a finding.

Remediation:

Configure the operating system to enforce a minimum 15-character password length. Add or modify the following line in the "/etc/security/pwquality.conf" file:

```
minlen = 15
```

References:

1. CIS Recommendation "Ensure password creation requirements are configured"

Additional Information:






CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-000205 The information system enforces minimum password length.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (i)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 <u>Use Unique Passwords</u> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

1.96 UBTU-22-611040 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must require the change of at least eight characters when passwords are changed.

```
GROUP ID: V-260566  
RULE ID: SV-260566r1015017
```

Rationale:

If the operating system allows the user to consecutively reuse extensive portions of passwords, this increases the chances of password compromise by increasing the window of opportunity for attempts at guessing and brute-force attacks.

The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. In other words, characters may be the same within the two passwords; however, the positions of the like characters must be different.

If the password length is an odd number then number of changed characters must be rounded up. For example, a password length of 15 characters must require the change of at least eight characters.

Audit:

Verify the operating system requires the change of at least eight characters when passwords are changed by using the following command:

```
$ grep -i difok /etc/security/pwquality.conf  
  
difok = 8
```

If "difok" is less than "8", is commented out, or is missing, this is a finding.

Remediation:

Configure the operating system to require the change of at least eight characters when passwords are changed.

Add or modify the following line in the "/etc/security/pwquality.conf" file:

```
difok = 8
```

References:

1. CIS Recommendation "Ensure the number of changed characters in a new password is configured"

Additional Information:






CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-000195 The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.

- NIST SP 800-53 :: IA-5 (1) (b)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (b)
- NIST SP 800-53A :: IA-5 (1).1 (v)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

1.97 UBTU-22-611045 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must be configured so that when passwords are changed or new passwords are established, pwquality must be used.

```
GROUP ID: V-260567
RULE ID: SV-260567r991587
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. "pwquality" enforces complex password construction configuration and has the ability to limit brute-force attacks on the system.

Audit:

Verify the operating system enforces password complexity rules by using the following command:

```
$ grep -i enforcing /etc/security/pwquality.conf
enforcing = 1
```

If "enforcing" is not "1", is commented out, or is missing, this is a finding. Check for the use of "pwquality" by using the following command:

```
$ cat /etc/pam.d/common-password | grep requisite | grep pam_pwquality
password      requisite      pam_pwquality.so retry=3
```

If "retry" is set to "0" or is greater than "3", or is missing, this is a finding.

Remediation:

Configure the operating system to enforce password complexity rules. Add or modify the following line in the "/etc/security/pwquality.conf" file:

```
enforcing = 1
```

Add or modify the following line in the "/etc/pam.d/common-password" file:

```
password requisite pam_pwquality.so retry=3
```






Note: The value of "retry" should be between "1" and "3".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

1.98 UBTU-22-611055 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must store only encrypted representations of passwords.

```
GROUP ID: V-260569
RULE ID: SV-260569r1044767
```

Rationale:

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. If the information system or application allows the user to consecutively reuse their password when that password has exceeded its defined lifetime, the end result is a password that is not changed as per policy requirements.

Audit:

Verify the operating system stores only encrypted representations of passwords with the following command:

```
$ grep pam_unix.so /etc/pam.d/common-password

password [success=1 default=ignore] pam_unix.so obscure sha512 shadow
remember=5 rounds=100000
```

If "sha512" is missing from the "pam_unix.so" line, this is a finding.

Remediation:

Configure the operating system to store encrypted representations of passwords. Add or modify the following line in the "/etc/pam.d/common-password" file:

```
password [success=1 default=ignore] pam_unix.so obscure sha512 shadow
remember=5 rounds=100000
```

Additional Information:






CCI-004062 For password-based authentication, store passwords using an approved salted key derivation function, preferably using a keyed hash.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (d)

CCI-000196 The information system, for password-based authentication, stores only cryptographically-protected passwords.

- NIST SP 800-53 :: IA-5 (1) (c)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (c)
- NIST SP 800-53A :: IA-5 (1).1 (v)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.			

1.99 UBTU-22-611060 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

The operating system must not allow accounts configured with blank or null passwords.

```
GROUP ID: V-260570  
RULE ID: SV-260570r1082233
```

Rationale:

If an account has an empty password, anyone could log on and run commands with the privileges of that account. Accounts with empty passwords must never be used in operational environments.

Audit:

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

```
$ grep nullok /etc/pam.d/common-auth /etc/pam.d/common-password
```

If this produces any output, this is a finding.

Remediation:

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

Remove any instances of the "nullok" option in "/etc/pam.d/common-auth" and "/etc/pam.d/common-password".

References:






1. CIS Recommendation "Ensure pam_unix does not include nullok"

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 <u>Use Unique Passwords</u> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

1.100 UBTU-22-611065 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

The operating system must not have accounts configured with blank or null passwords.

```
GROUP ID: V-260571  
RULE ID: SV-260571r991589
```

Rationale:

If an account has an empty password, anyone could log on and run commands with the privileges of that account. Accounts with empty passwords must never be used in operational environments.

Audit:

Verify all accounts on the system to have a password by using the following command:

```
$ sudo awk -F: '!!$2 {print $1}' /etc/shadow
```

If the command returns any results, this is a finding.

Remediation:

Configure all accounts on the system to have a password or lock the account by using the following commands:

Set the account password:

```
$ sudo passwd <username>
```

Or lock the account:

```
$ sudo passwd -l <username>
```

References:






1. CIS Recommendation "Ensure /etc/shadow password fields are not empty"

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 <u>Use Unique Passwords</u> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

1.101 UBTU-22-611070 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must encrypt all stored passwords with a FIPS 140-3-approved cryptographic hashing algorithm.

```
GROUP ID: V-260572
RULE ID: SV-260572r971535
```

Rationale:

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

Audit:

Verify that the shadow password suite configuration is set to encrypt passwords with a FIPS 140-3 approved cryptographic hashing algorithm by using the following command:

```
$ grep -i '^s*encrypt_method' /etc/login.defs

ENCRYPT_METHOD SHA512
```

If "ENCRYPT_METHOD" does not equal SHA512 or greater, is commented out, or is missing, this is a finding.

Remediation:

Configure the operating system to encrypt all stored passwords.
Add or modify the following line in the "/etc/login.defs" file:

```
ENCRYPT_METHOD SHA512
```

References:





1. CIS Recommendation "Ensure strong password hashing algorithm is configured"

Additional Information:

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53 :: IA-7
- NIST SP 800-53 Revision 4 :: IA-7
- NIST SP 800-53 Revision 5 :: IA-7
- NIST SP 800-53A :: IA-7.1

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.			

1.102 UBTU-22-612010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must implement multifactor authentication for remote access to privileged accounts in such a way that one of the factors is provided by a device separate from the system gaining access.

GROUP ID: V-260573 RULE ID: SV-260573r1015019
--

Rationale:

Using an authentication device, such as a CAC or token separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government personal identity verification card and the DOD common access card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000105-GPOS-00052, SRG-OS-000106-GPOS-00053, SRG-OS-000107-GPOS-00054, SRG-OS-000108-GPOS-00055

Audit:

Verify the operating system has the packages required for multifactor authentication installed by using the following command:

```
$ dpkg -l | grep libpam-pkcs11  
  
ii      libpam-pkcs11      0.6.11-4build2      amd64      Fully featured PAM  
module for using PKCS#11 smart cards
```

If the "libpam-pkcs11" package is not installed, this is a finding.

Remediation:

Install the "libpam-pkcs11" package by using the following command:

```
$ sudo apt-get install libpam-pkcs11
```

Additional Information:

CCI-000765 Implement multifactor authentication for network access to privileged accounts.

- NIST SP 800-53 :: IA-2 (1)
- NIST SP 800-53 Revision 4 :: IA-2 (1)
- NIST SP 800-53 Revision 5 :: IA-2 (1)
- NIST SP 800-53A :: IA-2 (1).1

CCI-000766 Implement multifactor authentication for network access to non-privileged accounts.

- NIST SP 800-53 :: IA-2 (2)
- NIST SP 800-53 Revision 4 :: IA-2 (2)
- NIST SP 800-53 Revision 5 :: IA-2 (2)
- NIST SP 800-53A :: IA-2 (2).1

CCI-004046 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

- NIST SP 800-53 Revision 5 :: IA-2 (6) (a)

CCI-004047 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that the device meets organization-defined strength of mechanism requirements.

- NIST SP 800-53 Revision 5 :: IA-2 (6) (b)

CCI-000767 The information system implements multifactor authentication for local access to privileged accounts.

- NIST SP 800-53 :: IA-2 (3)
- NIST SP 800-53 Revision 4 :: IA-2 (3)
- NIST SP 800-53A :: IA-2 (3).1









CCI-000768 The information system implements multifactor authentication for local access to non-privileged accounts.

- NIST SP 800-53 :: IA-2 (4)
- NIST SP 800-53 Revision 4 :: IA-2 (4)
- NIST SP 800-53A :: IA-2 (4).1

CCI-001948 The information system implements multifactor authentication for remote access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

- NIST SP 800-53 Revision 4 :: IA-2 (11)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.4 <u>Require MFA for Remote Network Access</u> Require MFA for remote network access.			
v8	6.5 <u>Require MFA for Administrative Access</u> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.			
v7	16.3 <u>Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.			

1.103 UBTU-22-612015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must accept personal identity verification (PIV) credentials.

```
GROUP ID: V-260574
RULE ID: SV-260574r958816
```

Rationale:

The use of PIV credentials facilitates standardization and reduces the risk of unauthorized access.

DOD has mandated the use of the common access card (CAC) to support identity management and personal authentication for systems covered under Homeland Security Presidential Directive (HSPD) 12, as well as making the CAC a primary component of layered protection for national security systems.

Audit:

Verify the "opensc-pkcs11" package is installed on the system by using the following command:

```
$ dpkg -l | grep opensc-pkcs11

ii      opensc-pkcs11:amd64      0.22.0-1Ubuntu2      amd64      Smart card
utilities with support for PKCS#15 compatible cards
```

If the "opensc-pkcs11" package is not installed, this is a finding.

Remediation:

Install the "opensc-pkcs11" package by using the following command:









```
$ sudo apt-get install opensc-pkcs11
```

Additional Information:

CCI-001953 Accepts Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4 :: IA-2 (12)
- NIST SP 800-53 Revision 5 :: IA-2 (12)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.4 <u>Require MFA for Remote Network Access</u> Require MFA for remote network access.			
v8	6.5 <u>Require MFA for Administrative Access</u> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.			
v7	16.3 <u>Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.			

1.104 UBTU-22-612020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must implement smart card logins for multifactor authentication for local and network access to privileged and nonprivileged accounts.

GROUP ID: V-260575 RULE ID: SV-260575r1044770
--

Rationale:

Without the use of multifactor authentication, the ease of access to privileged functions is greatly increased.

Multifactor authentication requires using two or more factors to achieve authentication.

Factors include:

1. Something a user knows (e.g., password/PIN);
2. Something a user has (e.g., cryptographic identification device, token); and
3. Something a user is (e.g., biometric).

A privileged account is defined as an information system account with authorizations of a privileged user.

Network access is defined as access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, or the internet).

The DOD common access card (CAC) with DOD-approved PKI is an example of multifactor authentication.

Satisfies: SRG-OS-000105-GPOS-00052, SRG-OS-000106-GPOS-00053, SRG-OS-000107-GPOS-00054, SRG-OS-000108-GPOS-00055

Audit:

Verify that the "pam_pkcs11.so" module is configured by using the following command:

```
$ grep -i pam_pkcs11.so /etc/pam.d/common-auth  
auth [success=3 default=ignore] pam_pkcs11.so
```

If "pam_pkcs11.so" is commented out or is missing, this is a finding.

Verify the sshd daemon allows public key authentication by using the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |  
tr '\n' ' ' | xargs sudo grep -iH 'pubkeyauthentication'  
  
/etc/ssh/sshd_config:PubkeyAuthentication yes
```

If "PubkeyAuthentication" is not set to "yes" or is commented out or missing, or if conflicting results are returned, this is a finding.

Remediation:

Configure the operating system to use multifactor authentication for access to accounts. Add or modify the following line in the "/etc/pam.d/common-auth" file:

```
auth [success=3 default=ignore] pam_pkcs11.so
```

Add or modify the following line in the "/etc/ssh/sshd_config" file:









```
PubkeyAuthentication yes
```

Additional Information:

CCI-000765 Implement multifactor authentication for network access to privileged accounts.

- NIST SP 800-53 :: IA-2 (1)
- NIST SP 800-53 Revision 4 :: IA-2 (1)
- NIST SP 800-53 Revision 5 :: IA-2 (1)
- NIST SP 800-53A :: IA-2 (1).1

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.4 <u>Require MFA for Remote Network Access</u> Require MFA for remote network access.			
v8	6.5 <u>Require MFA for Administrative Access</u> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.			
v7	16.3 <u>Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.			

1.105 UBTU-22-612025 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must electronically verify personal identity verification (PIV) credentials.

```
GROUP ID: V-260576
RULE ID: SV-260576r1069114
```

Rationale:

The use of PIV credentials facilitates standardization and reduces the risk of unauthorized access.

DOD has mandated the use of the common access card (CAC) to support identity management and personal authentication for systems covered under Homeland Security Presidential Directive (HSPD) 12, as well as making the CAC a primary component of layered protection for national security systems.

Audit:

Verify the operating system electronically verifies PIV credentials via certificate status checking by using the following command:

```
$ sudo grep use_pkcs11_module /etc/pam_pkcs11/pam_pkcs11.conf | sudo awk
'/pkcs11_module opensslc {/,/}/' /etc/pam_pkcs11/pam_pkcs11.conf | grep
cert_policy | grep ocspon

cert_policy = ca,signature,ocsp_on;
```

If every returned "cert_policy" line is not set to "ocsp_on", the line is commented out, or is missing, this is a finding.

Remediation:

Configure the operating system to do certificate status checking for multifactor authentication.

Add or modify all "cert_policy" lines in the "/etc/pam_pkcs11/pam_pkcs11.conf" file with the following:









```
ocsp_on
```


Additional Information:

CCI-001954 Electronically verifies Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4 :: IA-2 (12)
- NIST SP 800-53 Revision 5 :: IA-2 (12)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.4 <u>Require MFA for Remote Network Access</u> Require MFA for remote network access.			
v8	6.5 <u>Require MFA for Administrative Access</u> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.			
v7	16.3 <u>Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.			

1.106 UBTU-22-612030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system, for PKI-based authentication, must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.

```
GROUP ID: V-260577
RULE ID: SV-260577r1069112
```

Rationale:

Without path validation, an informed trust decision by the relying party cannot be made when presented with any certificate not already explicitly trusted.

A trust anchor is an authoritative entity represented via a public key and associated data. It is used in the context of public key infrastructures, X.509 digital certificates, and DNSSEC.

When there is a chain of trust, usually the top entity to be trusted becomes the trust anchor; it can be, for example, a certification authority (CA). A certification path starts with the subject certificate and proceeds through a number of intermediate certificates up to a trusted root certificate, typically issued by a trusted CA.

This requirement verifies that a certification path to an accepted trust anchor is used for certificate validation and that the path includes status information. Path validation is necessary for a relying party to make an informed trust decision when presented with any certificate not already explicitly trusted. Status information for certification paths includes certificate revocation lists or online certificate status protocol responses. Validation of the certificate status information is out of scope for this requirement.

Audit:

Verify the operating system, for PKI-based authentication, has valid certificates by constructing a certification path to an accepted trust anchor.

Determine which pkcs11 module is being used via the "use_pkcs11_module" in "/etc/pam_pkcs11/pam_pkcs11.conf" and then ensure "ca" is enabled in "cert_policy" by using the following command:

```
$ sudo grep use_pkcs11_module /etc/pam_pkcs11/pam_pkcs11.conf | sudo awk
'/pkcs11_module opensc {/,/}' /etc/pam_pkcs11/pam_pkcs11.conf | grep
cert_policy | grep ca

cert_policy = ca,signature,ocsp_on;
```

If "cert_policy" is not set to "ca", the line is commented out, or is missing, this is a finding.

Remediation:

Configure the operating system for PKI-based authentication, to validate certificates by constructing a certification path to an accepted trust anchor.

Add or modify all "cert_policy" lines in the "/etc/pam_pkcs11/pam_pkcs11.conf" file with the following:

```
cert_policy = ca,signature,ocsp_on;
```

Note: If the system is missing an "/etc/pam_pkcs11/" directory and an "/etc/pam_pkcs11/pam_pkcs11.conf", find an example to copy into place and modify accordingly at "/usr/share/doc/libpam-pkcs11/examples/pam_pkcs11.conf.example.gz".

Additional Information:









CCI-000185 For public key-based authentication, validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

- NIST SP 800-53 :: IA-5 (2)
- NIST SP 800-53 Revision 4 :: IA-5 (2) (a)
- NIST SP 800-53 Revision 5 :: IA-5 (2) (b) (1)
- NIST SP 800-53A :: IA-5 (2).1

CCI-004909 Include only approved trust anchors in trust stores or certificate stores managed by the organization.

- NIST SP 800-53 Revision 5 :: SC-17 b

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.4 <u>Require MFA for Remote Network Access</u> Require MFA for remote network access.			
v8	6.5 <u>Require MFA for Administrative Access</u> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.			
v7	16.3 <u>Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.			

1.107 UBTU-22-612035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system for PKI-based authentication, must implement a local cache of revocation data in case of the inability to access revocation information via the network.

```
GROUP ID: V-260578
RULE ID: SV-260578r1015021
```

Rationale:

Without configuring a local cache of revocation data, there is the potential to allow access to users who are no longer authorized (users with revoked certificates).

Audit:

Verify the operating system, , for PKI-based authentication, uses local revocation data when unable to access it from the network by using the following command:

Note: If smart card authentication is not being used on the system, this is not applicable.

```
$ grep cert_policy /etc/pam_pkcs11/pam_pkcs11.conf | grep -E --
'crl_auto|crl_offline'

cert_policy = ca,signature,ocsp_on,crl_auto;
```

If "cert_policy" is not set to include "crl_auto" or "crl_offline", is commented out, or is missing, this is a finding.

Remediation:

Configure the operating system, for PKI-based authentication, to use local revocation data when unable to access the network to obtain it remotely.

Add or update the "cert_policy" option in "/etc/pam_pkcs11/pam_pkcs11.conf" to include "crl_auto" or "crl_offline".

```
cert_policy = ca,signature,ocsp_on, crl_auto;
```









If the system is missing an "/etc/pam_pkcs11/" directory and an "/etc/pam_pkcs11/pam_pkcs11.conf", find an example to copy into place and modify accordingly at "/usr/share/doc/libpam-pkcs11/examples/pam_pkcs11.conf.example.gz".

Additional Information:

CCI-004068 For public key-based authentication, implement a local cache of revocation data to support path discovery and validation.

- NIST SP 800-53 Revision 5 :: IA-5 (2) (b) (2)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.4 <u>Require MFA for Remote Network Access</u> Require MFA for remote network access.			
v8	6.5 <u>Require MFA for Administrative Access</u> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.			
v7	16.3 <u>Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.			

1.108 UBTU-22-612040 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

The operating system must map the authenticated identity to the user or group account for PKI-based authentication.

GROUP ID: V-260579
RULE ID: SV-260579r958452

Rationale:

Without mapping the certificate used to authenticate to the user account, the ability to determine the identity of the individual user or group will not be available for forensic analysis.

Audit:

Verify that "use_mappers" is set to "pwent" in "/etc/pam_pkcs11/pam_pkcs11.conf" file by using the following command:

```
$ grep -i use_mappers /etc/pam_pkcs11/pam_pkcs11.conf  
  
use_mappers = pwent
```

If "use_mappers" does not contain "pwent", is commented out, or is missing, this is a finding.

Remediation:

Set "use_mappers=pwent" in "/etc/pam_pkcs11/pam_pkcs11.conf" or, if there is already a comma-separated list of mappers, add it to the list, separated by comma, and before the null mapper.









If the system is missing an "/etc/pam_pkcs11/" directory and an "/etc/pam_pkcs11/pam_pkcs11.conf", find an example to copy into place and modify accordingly at "/usr/share/doc/libpam-pkcs11/examples/pam_pkcs11.conf.example.gz".

Additional Information:

CCI-000187 For public key-based authentication, map the authenticated identity to the account of the individual or group.

- NIST SP 800-53 :: IA-5 (2)
- NIST SP 800-53 Revision 4 :: IA-5 (2) (c)
- NIST SP 800-53 Revision 5 :: IA-5 (2) (a) (2)
- NIST SP 800-53A :: IA-5 (2).1

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.4 <u>Require MFA for Remote Network Access</u> Require MFA for remote network access.			
v8	6.5 <u>Require MFA for Administrative Access</u> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.			
v7	16.3 <u>Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.			

1.109 UBTU-22-631010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must use DOD PKI-established certificate authorities for verification of the establishment of protected sessions.

```
GROUP ID: V-260580
RULE ID: SV-260580r958868
```

Rationale:

Untrusted certificate authorities (CA) can issue certificates, but they may be issued by organizations or individuals that seek to compromise DOD systems or by organizations with insufficient security controls. If the CA used for verifying the certificate is not a DOD-approved CA, trust of this CA has not been established.

The DOD will only accept PKI-certificates obtained from a DOD-approved internal or external certificate authority. Reliance on CAs for the establishment of secure sessions includes, for example, the use of SSL/TLS certificates.

Audit:

Verify the directory containing the root certificates for the operating system contains certificate files for DOD PKI-established certificate authorities by iterating over all files in the "/etc/ssl/certs" directory and checking if, at least one, has the subject matching "DOD ROOT CA".

```
$ ls /etc/ssl/certs | grep -i DOD
DOD_PKE_CA_chain.pem
```

If no DOD root certificate is found, this is a finding.

Verify that all root certificates present on the system have been approved by the AO.

```
$ ls /etc/ssl/certs
```

If a certificate is present that is not approved by the AO, this is a finding.

Remediation:

Configure the operating system to use of DOD PKI-established certificate authorities for verification of the establishment of protected sessions.

Add at least one DOD certificate authority to the "/usr/share/ca-certificates" directory in the CRT format.

Update the "/etc/ssl/certs" directory by using the following command:







```
$ sudo dpkg-reconfigure ca-certificates
```


Additional Information:

CCI-002470 Only allow the use of organization-defined certificate authorities for verification of the establishment of protected sessions.

- NIST SP 800-53 Revision 4 :: SC-23 (5)
- NIST SP 800-53 Revision 5 :: SC-23 (5)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.110 UBTU-22-631015 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must be configured such that Pluggable Authentication Module (PAM) prohibits the use of cached authentications after one day.

```
GROUP ID: V-260581
RULE ID: SV-260581r958828
```

Rationale:

If cached authentication information is out-of-date, the validity of the authentication information may be questionable.

Audit:

Verify that PAM prohibits the use of cached authentications after one day by using the following command:

Note: If smart card authentication is not being used on the system, this requirement is not applicable.

```
$ sudo grep -i '^s*offline_credentials_expiration' /etc/sss/sss.conf
/etc/sss/conf.d/*.conf

/etc/sss/sss.conf:offline_credentials_expiration = 1
```

If "offline_credentials_expiration" is not set to "1", is commented out, is missing, or conflicting results are returned, this is a finding.

Remediation:

Configure PAM to prohibit the use of cached authentications after one day. Add or modify the following line in the "/etc/sss/sss.conf" file, just below the line "[pam]":

```
offline_credentials_expiration = 1
```







Note: It is valid for this configuration to be in a file with a name that ends with ".conf" and does not begin with a "." in the "/etc/sss/conf.d/" directory instead of the "/etc/sss/sss.conf" file.

Additional Information:

CCI-002007 Prohibit the use of cached authenticators after an organization-defined time period.

- NIST SP 800-53 Revision 4 :: IA-5 (13)
- NIST SP 800-53 Revision 5 :: IA-5 (13)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.111 UBTU-22-651010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must use a file integrity tool to verify correct operation of all security functions.

```
GROUP ID: V-260582
RULE ID: SV-260582r958944
```

Rationale:

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

This requirement applies to the operating system performing security function verification/testing and/or systems and environments that require this functionality.

Audit:

Verify that Advanced Intrusion Detection Environment (AIDE) is installed by using the following command:

```
$ dpkg -l | grep aide

ii      aide      0.17.4-1      amd64      Advanced Intrusion Detection
Environment - dynamic binary
```

If AIDE is not installed, ask the system administrator how file integrity checks are performed on the system.

If there is no application installed to perform integrity checks, this is a finding.

Remediation:

Install the "aide" package:

```
$ sudo apt install aide
```

References:

1. CIS Recommendation "Ensure AIDE is installed"

Additional Information:

CCI-002696 Verify correct operation of organization-defined security functions.

- NIST SP 800-53 Revision 4 :: SI-6 a
- NIST SP 800-53 Revision 5 :: SI-6 a

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.14 <u>Log Sensitive Data Access</u> Log sensitive data access, including modification and disposal.			●
v7	14.9 <u>Enforce Detail Logging for Access or Changes to Sensitive Data</u> Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

1.112 UBTU-22-651015 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must configure AIDE to perform file integrity checking on the file system.

```
GROUP ID: V-260583
RULE ID: SV-260583r958944
```

Rationale:

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

This requirement applies to the operating system performing security function verification/testing and/or systems and environments that require this functionality.

Audit:

Verify that Advanced Intrusion Detection Environment (AIDE) is configured and operating correctly by using the following command (this will take a few minutes):

Note: If AIDE is not installed, this requirement is not applicable.

```
$ sudo aide -c /etc/aide/aide.conf --check
```

Example output:

```
Start timestamp: 2024-04-01 04:20:00 +1300 (AIDE 0.17.4)
AIDE found differences between database and filesystem!!
Ignored e2fs attributes: EIH
...
```

If AIDE is being used to perform file integrity checks but the command fails, this is a finding.

Remediation:

Initialize AIDE (this will take a few minutes):

```
$ sudo aideinit
```

```
Running aide --init..
```

Example output:

```
Start timestamp: 2024-04-01 04:20:00 +1300 (AIDE 0.17.4)
AIDE initialized database at /var/lib/aide/aide.db.new
Ignored e2fs attributes: EIh

Number of entries:          146185

-----
The attributes of the (uncompressed) database(s):
-----

/var/lib/aide/aide.db.new
SHA256      : UrYbC/KBOJcs8zKcSlKoifnnoPK66DEC
             Aw6odu/BpgY=
SHA512      : ezENbbuh937SPWvtsdjRzy3i47XjLg7j
             L3UGmr0EcGY6u8rczxgbn2RuwJfrIpef
             0clqMNobzrLXyDnnqEqAqw==
RMD160      : yBq2xio+g5ne4kvZzzMZ2v+EO9w=
TIGER       : GkJ/xkzJGu/aSQqk9A5LN271IOAQC3d0
CRC32       : g/beXA==
HAVAL       : zZm220YZiGna2edJ6Gi0rPv16AlpqeHB
             y/XLB3hIPEY=
WHIRLPOOL   : k6veoXavJ/BH9L125pCYAfTB8w5ZJkdC
             DvVmYS0+cgm7M0y/S2v42FNCEJ993mc
             3kZMXJR/VVmwKg/7ntGixQ==
GOST        : psjiyix6mJlNsE984D0NwbfgBmB0ETG1
             /R4PNvm/wKg=

End timestamp: 2024-04-01 04:29:16 +1300 (run time: 9m 16s)
```

References:

1. CIS Recommendation "Ensure AIDE is installed"

Additional Information:

CCI-002696 Verify correct operation of organization-defined security functions.

- NIST SP 800-53 Revision 4 :: SI-6 a
- NIST SP 800-53 Revision 5 :: SI-6 a

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.14 <u>Log Sensitive Data Access</u> Log sensitive data access, including modification and disposal.			●
v7	14.9 <u>Enforce Detail Logging for Access or Changes to Sensitive Data</u> Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

1.113 UBTU-22-651020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must notify designated personnel if baseline configurations are changed in an unauthorized manner. The file integrity tool must notify the system administrator when changes to the baseline configuration or anomalies in the operation of any security functions are discovered.

```
GROUP ID: V-260584
RULE ID: SV-260584r958794
```

Rationale:

Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the operating system. Changes to operating system configurations can have unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid unintended, negative consequences that could ultimately affect the security state of the operating system. The operating system's IMO/ISSO and SAs must be notified via email and/or monitoring system trap when there is an unauthorized modification of a configuration item.

Satisfies: SRG-OS-000363-GPOS-00150, SRG-OS-000447-GPOS-00201

Audit:

Verify that Advanced Intrusion Detection Environment (AIDE) notifies the system administrator when anomalies in the operation of any security functions are discovered by using the following command:

```
$ grep -i '^s*silentreports' /etc/default/aide
SILENTREPORTS=no
```

If "SILENTREPORTS" is set to "yes", is commented out, or is missing, this is a finding.

Remediation:

Configure AIDE to notify designated personnel if baseline configurations are changed in an unauthorized manner.

Add or modify the following line in the "/etc/default/aide" file:

```
SILENTREPORTS=no
```

Additional Information:

CCI-001744 Implement organization-defined security responses automatically if baseline configurations are changed in an unauthorized manner.

1. NIST SP 800-53 Revision 4 :: CM-3 (5)
2. NIST SP 800-53 Revision 5 :: CM-3 (5)

CCI-002702 Shut the system down, restart the system, and/or initiate organization-defined alternative action(s) when anomalies in the operation of the organization-defined security functions are discovered.

- NIST SP 800-53 Revision 4 :: SI-6 d
- NIST SP 800-53 Revision 5 :: SI-6 d

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.14 <u>Log Sensitive Data Access</u> Log sensitive data access, including modification and disposal.			●
v7	14.9 <u>Enforce Detail Logging for Access or Changes to Sensitive Data</u> Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

1.114 UBTU-22-651025 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must be configured so that the script that runs each 30 days or less to check file integrity is the default.

```
GROUP ID: V-260585
RULE ID: SV-260585r958946
```

Rationale:

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

Notifications provided by information systems include, for example, electronic alerts to system administrators, messages to local computer consoles, and/or hardware indications, such as lights.

This requirement applies to the operating system performing security function verification/testing and/or systems and environments that require this functionality.

Audit:

Verify that the Advanced Intrusion Detection Environment (AIDE) default script used to check file integrity each 30 days or less is unchanged.

Download the original aide-common package in the /tmp directory:

```
$ cd /tmp; apt download aide-common
```

Fetch the SHA1 of the original script file:

```
$ dpkg-deb --fsys-tarfile /tmp/aide-common_*.deb | tar -xO
./usr/share/aide/config/cron.daily/aide | shasum
b71bb2cafaedf15ec3ac2f566f209d3260a37af0 -
```

Compare with the SHA1 of the file in the daily or monthly cron directory:

```
$ shasum /etc/cron.{daily,monthly}/aide 2>/dev/null
```

```
b71bb2cafaedf15ec3ac2f566f209d3260a37af0 /etc/cron.daily/aide
```

If there is no AIDE script file in the cron directories, or the SHA1 value of at least one file in the daily or monthly cron directory does not match the SHA1 of the original, this is a finding.

Remediation:

The cron file for AIDE is fairly complex as it creates the report. This file is installed with the "aide-common" package, and the default can be restored by copying it from the package:

Extract the aide script from the "aide-common" package to its original place:

```
$ dpkg-deb --fsys-tarfile /tmp/aide-common_*.deb | sudo tar -x
./usr/share/aide/config/cron.daily/aide -C /
```

Copy it to the cron.daily directory:







```
$ sudo cp -f /usr/share/aide/config/cron.daily/aide /etc/cron.daily/aide
```

Additional Information:

CCI-002699 Perform verification of the correct operation of organization-defined security functions: when the system is in an organization-defined transitional state; upon command by a user with appropriate privileges; and/or on an organization-defined frequency.

- NIST SP 800-53 Revision 4 :: SI-6 b
- NIST SP 800-53 Revision 5 :: SI-6 b

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.115 UBTU-22-651030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must use cryptographic mechanisms to protect the integrity of audit tools.

GROUP ID: V-260586 RULE ID: SV-260586r1069107
--

Rationale:

Protecting the integrity of the tools used for auditing purposes is a critical step toward ensuring the integrity of audit information. Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

It is not uncommon for attackers to replace the audit tools or inject code into the existing tools with the purpose of providing the capability to hide or erase system activity from the audit logs.

To address this risk, audit tools must be cryptographically signed in order to provide the capability to identify when the audit tools have been modified, manipulated, or replaced. An example is a checksum hash of the file or files.

Audit:

Verify that Advanced Intrusion Detection Environment (AIDE) is properly configured to use cryptographic mechanisms to protect the integrity of audit tools by using the following command:

```
$ grep -E '(\sbin\/(audit|au))' /etc/aide/aide.conf

/sbin/auditctl p+i+n+u+g+s+b+acl+xattrs+sha512
/sbin/auditd p+i+n+u+g+s+b+acl+xattrs+sha512
/sbin/aureport p+i+n+u+g+s+b+acl+xattrs+sha512
/sbin/aureport p+i+n+u+g+s+b+acl+xattrs+sha512
/sbin/auditd p+i+n+u+g+s+b+acl+xattrs+sha512
/sbin/auditd p+i+n+u+g+s+b+acl+xattrs+sha512
```

If any of the lines do not appear as shown, are commented out, or are missing, this is a finding.

Remediation:

Configure AIDE to protect the integrity of audit tools:

Add or modify the following lines in the "/etc/aide/aide.conf" file:

```
# Audit Tools
/sbin/auditctl p+i+n+u+g+s+b+acl+xattrs+sha512
/sbin/auditd p+i+n+u+g+s+b+acl+xattrs+sha512
/sbin/ausearch p+i+n+u+g+s+b+acl+xattrs+sha512
/sbin/aureport p+i+n+u+g+s+b+acl+xattrs+sha512
/sbin/autrace p+i+n+u+g+s+b+acl+xattrs+sha512
/sbin/augenrules p+i+n+u+g+s+b+acl+xattrs+sha512
```

References:

1. CIS Recommendation "Ensure cryptographic mechanisms are used to protect the integrity of audit tools"

Additional Information:

CCI-001496 Implement cryptographic mechanisms to protect the integrity of audit tools.

- NIST SP 800-53 :: AU-9 (3)
- NIST SP 800-53 Revision 4 :: AU-9 (3)
- NIST SP 800-53 Revision 5 :: AU-9 (3)
- NIST SP 800-53A :: AU-9 (3).1

1.116 UBTU-22-651035 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must have a crontab script running weekly to offload audit events of standalone systems.

```
GROUP ID: V-260587
RULE ID: SV-260587r959008
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Offloading is a common process in information systems with limited audit storage capacity.

Audit:

Verify there is a script that offloads audit data and that script runs weekly by using the following command:

Note: If the system is not connected to a network, this requirement is not applicable.

```
$ ls /etc/cron.weekly
<audit_offload_script_name>
```

Check if the script inside the file does offloading of audit logs to external media. If the script file does not exist or does not offload audit logs, this is a finding.

Remediation:

Create a script that offloads audit logs to external media and runs weekly.








The script must be located in the "/etc/cron.weekly" directory.

Additional Information:

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4 :: AU-4 (1)
- NIST SP 800-53 Revision 5 :: AU-4 (1)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.1 <u>Establish and Maintain an Audit Log Management Process</u> Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	6.4 <u>Ensure adequate storage for logs</u> Ensure that all systems that store logs have adequate storage space for the logs generated.			
v7	6.5 <u>Central Log Management</u> Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.			

1.117 UBTU-22-652010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must be configured to preserve log records from failure events.

```
GROUP ID: V-260588
RULE ID: SV-260588r991562
```

Rationale:

Failure to a known state can address safety or security in accordance with the mission/business needs of the organization. Failure to a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system.

Preserving operating system state information helps to facilitate operating system restart and return to the operational mode of the organization with least disruption to mission/business processes.

Audit:

Verify the log service is installed properly by using the following command:

```
$ dpkg -l | grep rsyslog

ii      rsyslog      8.2112.0-2ubuntu2.2      amd64      reliable system and
kernel logging daemon
```

If the "rsyslog" package is not installed, this is a finding.

Check that the log service is enabled and active by using the following commands:

```
$ systemctl is-enabled rsyslog.service

enabled
$ systemctl is-active rsyslog.service

active
```

If "rsyslog.service" is not enabled and active, this is a finding.

Remediation:

Install the log service by using the following command:

```
$ sudo apt-get install rsyslog
```

Enable and activate the log service by using the following command:

```
$ sudo systemctl enable rsyslog.service --now
```

References:









1. CIS Recommendations "Ensure rsyslog is installed" & "Ensure rsyslog service is enabled and active"

Additional Information:

CCI-001665 Preserve organization-defined system state information in the event of a system failure.

- NIST SP 800-53 :: SC-24
- NIST SP 800-53 Revision 4 :: SC-24
- NIST SP 800-53 Revision 5 :: SC-24
- NIST SP 800-53A :: SC-24.1 (v)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

1.118 UBTU-22-652015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must monitor remote access methods.

GROUP ID: V-260589
RULE ID: SV-260589r958406

Rationale:

Remote access services, such as those providing remote access to network devices and information systems, which lack automated monitoring capabilities, increase risk and make remote user access management difficult at best.

Remote access is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Automated monitoring of remote access sessions allows organizations to detect cyberattacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote access capabilities, such as Remote Desktop Protocol (RDP), on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

Audit:

Verify that the operating system monitors all remote access methods by using the following command:

```
$ grep -Er '^(auth\.\\*,authpriv\.\\*|daemon\.\\*)' /etc/rsyslog.*  
  
/etc/rsyslog.d/50-default.conf:auth.*,authpriv.* /var/log/secure  
/etc/rsyslog.d/50-default.conf:daemon.* /var/log/messages
```

If "auth.", "authpriv.", or "daemon.*" are not configured to be logged in at least one of the config files, this is a finding.

Remediation:

Configure the operating system to monitor all remote access methods.
Add or modify the following line in the "/etc/rsyslog.d/50-default.conf" file:

```
auth.*,authpriv.* /var/log/secure  
daemon.* /var/log/messages
```

Restart "rsyslog.service" for the changes to take effect by using the following command:







```
$ sudo systemctl restart rsyslog.service
```

Additional Information:

CCI-000067 Employ automated mechanisms to monitor remote access methods.

- NIST SP 800-53 :: AC-17 (1)
- NIST SP 800-53 Revision 4 :: AC-17 (1)
- NIST SP 800-53 Revision 5 :: AC-17 (1)
- NIST SP 800-53A :: AC-17 (1).1

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.119 UBTU-22-653010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must have the "auditd" package installed.

GROUP ID: V-260590 RULE ID: SV-260590r1015022
--

Rationale:

Without establishing the when, where, type, source, and outcome of events that occurred, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

Successful incident response and auditing relies on timely, accurate system information and analysis in order to allow the organization to identify and respond to potential incidents in a proficient manner. If the operating system does not provide the ability to centrally review the operating system logs, forensic analysis is negatively impacted.

Associating event types with detected events in the operating system audit logs provides a means of investigating an attack; recognizing resource utilization or capacity thresholds; or identifying an improperly configured operating system.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000038-GPOS-00016, SRG-OS-000039-GPOS-00017, SRG-OS-000040-GPOS-00018, SRG-OS-000041-GPOS-00019, SRG-OS-000042-GPOS-00020, SRG-OS-000042-GPOS-00021, SRG-OS-000051-GPOS-00024, SRG-OS-000054-GPOS-00025, SRG-OS-000062-GPOS-00031, SRG-OS-000122-GPOS-00063, SRG-OS-000337-GPOS-00129, SRG-OS-000348-GPOS-00136, SRG-OS-000349-GPOS-00137, SRG-OS-000350-GPOS-00138, SRG-OS-000351-GPOS-00139, SRG-OS-000352-GPOS-00140, SRG-OS-000353-GPOS-00141, SRG-OS-000354-GPOS-00142, SRG-OS-000365-GPOS-00152, SRG-OS-000475-GPOS-00220

Audit:

Verify the "auditd" package is installed by using the following command:

```
$ dpkg -l | grep auditd  
  
ii      libauditd      1:3.0.7-1build1      amd64      User space tools for  
security auditing
```

If the "auditd" package is not installed, this is a finding.

Remediation:

Install the "auditd" package by using the following command:

```
$ sudo apt-get install auditd
```

References:

1. CIS Recommendation "Ensure auditd packages are installed"

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000131 Ensure that audit records containing information that establishes when the event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 b
- NIST SP 800-53A :: AU-3.1

CCI-000132 Ensure that audit records containing information that establishes where the event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 c
- NIST SP 800-53A :: AU-3.1

CCI-000133 Ensure that audit records containing information that establishes the source of the event.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 d
- NIST SP 800-53A :: AU-3.1
-

CCI-000134 Ensure that audit records containing information that establishes the outcome of the event.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 e
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)
-

CCI-000154 Provide the capability to centrally review and analyze audit records from multiple components within the system.

- NIST SP 800-53 :: AU-6 (4)
- NIST SP 800-53 Revision 4 :: AU-6 (4)
- NIST SP 800-53 Revision 5 :: AU-6 (4)
- NIST SP 800-53A :: AU-6 (4).1
-

CCI-000158 Provide the capability to process, sort, and search audit records for events of interest based on organization-defined audit fields within audit records.

- NIST SP 800-53 :: AU-7 (1)
- NIST SP 800-53 Revision 4 :: AU-7 (1)
- NIST SP 800-53 Revision 5 :: AU-7 (1)
- NIST SP 800-53A :: AU-7 (1).1

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)
-

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5 :: CM-5 (1) (b)

CCI-001875 Provide an audit reduction capability that supports on-demand audit review and analysis.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001876 Provide an audit reduction capability that supports on-demand reporting requirements.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001877 Provide an audit reduction capability that supports after-the-fact investigations of incidents.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001878 Provide a report generation capability that supports on-demand audit review and analysis.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001879 Provide a report generation capability that supports on-demand reporting requirements.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001880 Provide a report generation capability that supports after-the-fact investigations of security incidents.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001881 Provide an audit reduction capability that does not alter original content or time ordering of audit records.

- NIST SP 800-53 Revision 4 :: AU-7 b
- NIST SP 800-53 Revision 5 :: AU-7 b

CCI-001882 Provide a report generation capability that does not alter original content or time ordering of audit records.

- NIST SP 800-53 Revision 4 :: AU-7 b
- NIST SP 800-53 Revision 5 :: AU-7 b






CCI-001914 Provide the capability for organization-defined individuals or roles to change the logging to be performed on organization-defined system components based on organization-defined selectable event criteria within organization-defined time thresholds.

- NIST SP 800-53 Revision 4 :: AU-12 (3)
- NIST SP 800-53 Revision 5 :: AU-12 (3)

CCI-001814 The Information system supports auditing of the enforcement actions.

- NIST SP 800-53 Revision 4 :: CM-5 (1)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

1.120 UBTU-22-653015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must produce audit records and reports containing information to establish when, where, what type, the source, and the outcome for all DOD-defined auditable events and actions in near real time.

GROUP ID: V-260591 RULE ID: SV-260591r1015023
--

Rationale:

Without establishing the when, where, type, source, and outcome of events that occurred, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

Successful incident response and auditing relies on timely, accurate system information and analysis to allow the organization to identify and respond to potential incidents in a proficient manner. If the operating system does not provide the ability to centrally review the operating system logs, forensic analysis is negatively impacted.

Associating event types with detected events in the operating system audit logs provides a means of investigating an attack; recognizing resource utilization or capacity thresholds; or identifying an improperly configured operating system.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000038-GPOS-00016, SRG-OS-000039-GPOS-00017, SRG-OS-000040-GPOS-00018, SRG-OS-000041-GPOS-00019, SRG-OS-000042-GPOS-00020, SRG-OS-000042-GPOS-00021, SRG-OS-000051-GPOS-00024, SRG-OS-000054-GPOS-00025, SRG-OS-000062-GPOS-00031, SRG-OS-000122-GPOS-00063, SRG-OS-000337-GPOS-00129, SRG-OS-000348-GPOS-00136, SRG-OS-000349-GPOS-00137, SRG-OS-000350-GPOS-00138, SRG-OS-000351-GPOS-00139, SRG-OS-000352-GPOS-00140, SRG-OS-000353-GPOS-00141, SRG-OS-000354-GPOS-00142, SRG-OS-000365-GPOS-00152, SRG-OS-000475-GPOS-00220

Audit:

Verify the "auditd.service" is enabled and active by using the following commands:

```
$ systemctl is-enabled auditd.service  
  
enabled  
$ systemctl is-active auditd.service  
  
active
```

If the "auditd.service" is not enabled and active, this is a finding.

Remediation:

Verify the "auditd.service" is enabled and active by using the following commands:

```
$ systemctl is-enabled auditd.service  
  
enabled  
$ systemctl is-active auditd.service  
  
active
```

If the "auditd.service" is not enabled and active, this is a finding.

Enable and start the "auditd.service" by using the following command:

```
$ sudo systemctl enable auditd.service --now
```

References:

1. CIS Recommendation "Ensure auditd service is enabled and active"

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000131 Ensure that audit records containing information that establishes when the event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 b
- NIST SP 800-53A :: AU-3.1

CCI-000132 Ensure that audit records containing information that establishes where the event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 c
- NIST SP 800-53A :: AU-3.1

CCI-000133 Ensure that audit records containing information that establishes the source of the event.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 d
- NIST SP 800-53A :: AU-3.1

CCI-000134 Ensure that audit records containing information that establishes the outcome of the event.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 e
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)
-

CCI-000154 Provide the capability to centrally review and analyze audit records from multiple components within the system.

- NIST SP 800-53 :: AU-6 (4)
- NIST SP 800-53 Revision 4 :: AU-6 (4)
- NIST SP 800-53 Revision 5 :: AU-6 (4)
- NIST SP 800-53A :: AU-6 (4).1

CCI-000158 Provide the capability to process, sort, and search audit records for events of interest based on organization-defined audit fields within audit records.

- NIST SP 800-53 :: AU-7 (1)
- NIST SP 800-53 Revision 4 :: AU-7 (1)
- NIST SP 800-53 Revision 5 :: AU-7 (1)
- NIST SP 800-53A :: AU-7 (1).1

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5 :: CM-5 (1) (b)

CCI-001875 Provide an audit reduction capability that supports on-demand audit review and analysis.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001876 Provide an audit reduction capability that supports on-demand reporting requirements.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001877 Provide an audit reduction capability that supports after-the-fact investigations of incidents.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001878 Provide a report generation capability that supports on-demand audit review and analysis.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001879 Provide a report generation capability that supports on-demand reporting requirements.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001880 Provide a report generation capability that supports after-the-fact investigations of security incidents.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001881 Provide an audit reduction capability that does not alter original content or time ordering of audit records.

- NIST SP 800-53 Revision 4 :: AU-7 b
- NIST SP 800-53 Revision 5 :: AU-7 b

CCI-001882 Provide a report generation capability that does not alter original content or time ordering of audit records.

- NIST SP 800-53 Revision 4 :: AU-7 b
- NIST SP 800-53 Revision 5 :: AU-7 b









CCI-001914 Provide the capability for organization-defined individuals or roles to change the logging to be performed on organization-defined system components based on organization-defined selectable event criteria within organization-defined time thresholds.

- NIST SP 800-53 Revision 4 :: AU-12 (3)
- NIST SP 800-53 Revision 5 :: AU-12 (3)

CCI-001814 The Information system supports auditing of the enforcement actions.

- NIST SP 800-53 Revision 4 :: CM-5 (1)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

1.121 UBTU-22-653020 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system audit event multiplexor must be configured to offload audit logs onto a different system from the system being audited.

```
GROUP ID: V-260592
RULE ID: SV-260592r958754
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Offloading is a common process in information systems with limited audit storage capacity.

The auditd service does not include the ability to send audit records to a centralized server for management directly. However, it can use a plug-in for audit event multiplexor to pass audit records to a remote server.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Audit:

Verify the audit event multiplexor is configured to offload audit records to a different system from the system being audited.

Check if the "audispd-plugins" package is installed:

```
$ dpkg -l | grep audispd-plugins

ii      audispd-plugins      1:3.0.7-1build1      amd64      Plugins for the
audit event dispatcher
```

If the "audispd-plugins" package is not installed, this is a finding.

Check that the records are being offloaded to a remote server by using the following command:

```
$ sudo grep -i active /etc/audit/plugins.d/au-remote.conf

active = yes
```

If "active" is not set to "yes", or the line is commented out, or is missing, this is a finding.

Check that audisp-remote plugin is configured to send audit logs to a different system:

```
$ sudo grep -i remote_server /etc/audit/audisp-remote.conf  
remote_server = 240.9.19.81
```

If the "remote_server" parameter is not set, is set with a local IP address, or is set with an invalid IP address, this is a finding.

Remediation:

Configure the audit event multiplexor to offload audit records to a different system from the system being audited.

Install the "audisp-plugins" package by using the following command:

```
$ sudo apt-get install audispd-plugins
```

Set the audisp-remote plugin as active by editing the "/etc/audit/plugins.d/audisp-remote.conf" file:

```
$ sudo sed -i -E 's/active\s*=\s*no/active = yes/' /etc/audit/plugins.d/audisp-remote.conf
```

Set the IP address of the remote system by editing the "/etc/audit/audisp-remote.conf" file:

```
$ sudo sed -i -E 's/(remote_server\s*=).*\/\1 <remote_server_ip_address>/' /etc/audit/audisp-remote.conf
```

Restart the "auditd.service" for the changes to take effect:









```
$ sudo systemctl restart auditd.service
```

Additional Information:

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4 :: AU-4 (1)
- NIST SP 800-53 Revision 5 :: AU-4 (1)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

1.122 UBTU-22-653025 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must alert the information system security officer (ISSO) and system administrator (SA) in the event of an audit processing failure.

```
GROUP ID: V-260593
RULE ID: SV-260593r958424
```

Rationale:

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Audit:

Verify that the SA and ISSO are notified in the event of an audit processing failure by using the following command:

Note: An email package must be installed on the system for email notifications to be sent.

```
$ sudo grep -i action_mail_acct /etc/audit/auditd.conf

action_mail_acct = <administrator_email_account>
```

If "action_mail_acct" is not set to the email address of the SA and/or ISSO, is commented out, or is missing, this is a finding.

Remediation:

Configure "auditd" service to notify the SA and ISSO in the event of an audit processing failure.

Add or modify the following line in the "/etc/audit/auditd.conf " file:

```
action_mail_acct = <administrator_email_account>
```

Note: Change "administrator_email_account" to the email address of the SA and/or ISSO.

Restart the "auditd" service for the changes take effect:

```
$ sudo systemctl restart auditd.service
```

References:

1. CIS Recommendation "Ensure system is disabled when audit logs are full"

Additional Information:

CCI-000139 Alert organization-defined personnel or roles within an organization-defined time period in the event of an audit logging process failure.

- NIST SP 800-53 :: AU-5 a
- NIST SP 800-53 Revision 4 :: AU-5 a
- NIST SP 800-53 Revision 5 :: AU-5 a
- NIST SP 800-53A :: AU-5.1 (ii)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 <u>Ensure adequate storage for logs</u> Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

1.123 UBTU-22-653030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must shut down by default upon audit failure.

```
GROUP ID: V-260594
RULE ID: SV-260594r1038966
```

Rationale:

It is critical that when the operating system is at risk of failing to process audit logs as required, it takes action to mitigate the failure. Audit processing failures include: software/hardware errors; failures in the audit capturing mechanisms; and audit storage capacity being reached or exceeded. Responses to audit failure depend upon the nature of the failure mode.

When availability is an overriding concern, other approved actions in response to an audit failure are as follows:

1. If the failure was caused by the lack of audit record storage capacity, the operating system must continue generating audit records if possible (automatically restarting the audit service if necessary), overwriting the oldest audit records in a first-in-first-out manner.
2. If audit records are sent to a centralized collection server and communication with this server is lost or the server fails, the operating system must queue audit records locally until communication is restored or until the audit records are retrieved manually. Upon restoration of the connection to the centralized collection server, action should be taken to synchronize the local audit data with the collection server.

Audit:

Verify that the operating system takes the appropriate action when the audit storage volume is full by using the following command:

```
$ sudo grep -i disk_full_action /etc/audit/auditd.conf

disk_full_action = HALT
```

If "disk_full_action" is not set to "HALT", "SYSLOG", or "SINGLE", is commented out, or is missing, this is a finding.

Remediation:

Configure the operating system to shut down by default upon audit failure. Add or modify the following line in the "/etc/audit/auditd.conf " file:

```
disk_full_action = HALT
```

Restart the "auditd" service for the changes to take effect:

```
$ sudo systemctl restart auditd.service
```

Note: If system availability has been determined to be more important, and this decision is documented with the ISSO, configure Ubuntu 22.04 LTS to notify system administration staff and ISSO staff in the event of an audit processing failure by setting the "disk_full_action" to "SYSLOG" or "SINGLE".

References:









1. CIS Recommendation "Ensure system is disabled when audit logs are full"

Additional Information:

CCI-000140 Take organization-defined actions upon audit failure include, shutting down the system, overwriting oldest audit records, and stopping the generation of audit records.

- NIST SP 800-53 :: AU-5 b
- NIST SP 800-53 Revision 4 :: AU-5 b
- NIST SP 800-53 Revision 5 :: AU-5 b
- NIST SP 800-53A :: AU-5.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	6.4 <u>Ensure adequate storage for logs</u> Ensure that all systems that store logs have adequate storage space for the logs generated.			

1.124 UBTU-22-653035 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must allocate audit record storage capacity to store at least one weeks' worth of audit records, when audit records are not immediately sent to a central audit record storage facility.

```
GROUP ID: V-260595
RULE ID: SV-260595r958752
```

Rationale:

To ensure operating systems have a sufficient storage capacity in which to write the audit logs, operating systems must be able to allocate audit record storage capacity.

The task of allocating audit record storage capacity is usually performed during initial installation of the operating system.

Audit:

allocates audit record storage capacity to store at least one week's worth of audit records when audit records are not immediately sent to a central audit record storage facility.

Determine which partition the audit records are being written to by using the following command:

```
$ sudo grep -i log_file /etc/audit/auditd.conf

log_file = /var/log/audit/audit.log
```

Check the size of the partition that audit records are written to (with the example being "/var/log/audit/") by using the following command:

```
$ sudo df -h /var/log/audit/

/dev/sda2 24G 10.4G 13.6G 43% /var/log/audit
```

If the audit records are not written to a partition made specifically for audit records ("/var/log/audit" as a separate partition), determine the amount of space being used by other files in the partition by using the following command:

```
$ sudo du -sh <audit_partition>

1.8G /var/log/audit
```


Note: The partition size needed to capture a week's worth of audit records is based on the activity level of the system and the total storage capacity available.
If the audit record partition is not allocated for sufficient storage capacity, this is a finding.

Remediation:

Allocate enough storage capacity for at least one week's worth of audit records when audit records are not immediately sent to a central audit record storage facility.
If audit records are stored on a partition made specifically for audit records, use the "parted" program to resize the partition with sufficient space to contain one week's worth of audit records.
If audit records are not stored on a partition made specifically for audit records, a new partition with sufficient amount of space will need be to be created.
Set the auditd server to point to the mount point where the audit records must be located:

```
$ sudo sed -i -E 's@^(log_file\s*=\s*)\..*@\\1<audit_partition_mountpoint>/audit.log@' /etc/audit/auditd.conf
```






where <audit_partition_mountpoint> is the aforementioned mount point.

Additional Information:

CCI-001849 Allocate audit log storage capacity to accommodate organization-defined audit record retention requirements.

- NIST SP 800-53 Revision 4 :: AU-4
- NIST SP 800-53 Revision 5 :: AU-4

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	6.4 <u>Ensure adequate storage for logs</u> Ensure that all systems that store logs have adequate storage space for the logs generated.			

1.125 UBTU-22-653040 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must immediately notify the system administrator (SA) and information system security officer (ISSO) when the audit record storage volume reaches 25 percent remaining of the allocated capacity.

```
GROUP ID: V-260596
RULE ID: SV-260596r971542
```

Rationale:

If security personnel are not notified immediately when storage volume reaches 25 percent remaining of the allocated capacity, they are unable to plan for audit record storage capacity expansion.

Audit:

Verify the operating system is configured to notify the SA and ISSO when the audit record storage volume reaches 25 percent remaining of the allocated capacity by using the following command:

```
$ sudo grep -i space_left /etc/audit/auditd.conf

space_left = 25%
space_left_action = email
```

If "space_left" is set to a value less than "25%", is commented out, or is missing, this is a finding.

If "space_left_action" is not set to "email", is commented out, or is missing, this is a finding.

Note: If the "space_left_action" is set to "exec", the system executes a designated script. If this script informs the SA of the event, this is not a finding.

Remediation:

Configure the operating system to notify the SA and ISSO when the audit record storage volume reaches 25 percent remaining of the allocated capacity.

Add or modify the following lines in the "/etc/audit/auditd.conf" file:

```
space_left = 25%
space_left_action = email
```

Restart the "auditd" service for the changes to take effect:

```
$ sudo systemctl restart auditd.service
```









Note: If the "space_left_action" parameter is set to "exec", ensure the command being executed notifies the SA and ISSO.

Additional Information:

CCI-001855 Provide a warning to organization-defined personnel, roles, and/or locations within an organization-defined time period when allocated audit log storage volume reaches an organization-defined percentage of repository maximum audit log storage capacity.

- NIST SP 800-53 Revision 4 :: AU-5 (1)
- NIST SP 800-53 Revision 5 :: AU-5 (1)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	6.4 <u>Ensure adequate storage for logs</u> Ensure that all systems that store logs have adequate storage space for the logs generated.			

1.126 UBTU-22-653045 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must be configured so that audit log files are not read- or write-accessible by unauthorized users.

```
GROUP ID: V-260597
RULE ID: SV-260597r958434
```

Rationale:

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit operating system activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028

Audit:

Verify that the audit log files have a mode of "600" or less permissive.
Determine where the audit logs are stored by using the following command:

```
$ sudo grep -iw log_file /etc/audit/auditd.conf

log_file = /var/log/audit/audit.log
```

Using the path of the directory containing the audit logs, determine if the audit log files have a mode of "600" or less by using the following command:

```
$ sudo stat -c "%n %a" /var/log/audit/*

/var/log/audit/audit.log 600
```

If the audit log files have a mode more permissive than "600", this is a finding.

Remediation:

Configure the audit log files to have a mode of "600" or less permissive.
Using the path of the directory containing the audit logs, configure the audit log files to have a mode of "600" or less permissive by using the following command:

```
$ sudo chmod 600 /var/log/audit/*
```

References:

1. CIS Recommendation "Ensure audit log files mode is configured"

Additional Information:







CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CIS Controls:

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

1.127 UBTU-22-653050 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must be configured to permit only authorized users ownership of the audit log files.

```
GROUP ID: V-260598
RULE ID: SV-260598r958434
```

Rationale:

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit operating system activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Verify the audit log files are owned by "root" account.

Determine where the audit logs are stored by using the following command:

```
$ sudo grep -iw log_file /etc/audit/auditd.conf

log_file = /var/log/audit/audit.log
```

Using the path of the directory containing the audit logs, determine if the audit log files are owned by the "root" user by using the following command:

```
$ sudo stat -c "%n %U" /var/log/audit/*

/var/log/audit/audit.log root
```

If the audit log files are owned by a user other than "root", this is a finding.

Remediation:

Configure the audit log directory and its underlying files to be owned by "root" user.

Using the path of the directory containing the audit logs, configure the audit log files to be owned by "root" user by using the following command:

```
$ sudo chown root /var/log/audit/*
```

References:

1. CIS Recommendation "Ensure audit log files owner is configured"

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1







CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CIS Controls:

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

1.128 UBTU-22-653055 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must permit only authorized groups ownership of the audit log files.

```
GROUP ID: V-260599
RULE ID: SV-260599r958434
```

Rationale:

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit operating system activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Verify the group owner of newly created audit logs is "root" by using the following command:

```
$ sudo grep -iw log_group /etc/audit/auditd.conf

log_group = root
```

If "log_group" is not set to "root", this is a finding.

Remediation:

Configure the group owner of newly created audit logs to be "root".
Add or modify the following lines in the "/etc/audit/auditd.conf " file:

```
log_group = root
```

Reload the configuration file of the audit service to update the group ownership of existing files:

```
$ sudo systemctl kill auditd -s SIGHUP
```

References:

1. CIS Recommendation "Ensure audit log files group owner is configured"

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1







CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CIS Controls:

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

1.129 UBTU-22-653060 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must be configured so that the audit log directory is not write-accessible by unauthorized users.

```
GROUP ID: V-260600
RULE ID: SV-260600r958438
```

Rationale:

If audit information were to become compromised, then forensic analysis and discovery of the true source of potentially malicious system activity is impossible to achieve.

To ensure the veracity of audit information, the operating system must protect audit information from unauthorized deletion. This requirement can be achieved through multiple methods, which will depend upon system architecture and design.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit information system activity.

Audit:

Verify that the audit log directory has a mode of "750" or less permissive.
Determine where the audit logs are stored by using the following command:

```
$ sudo grep -iw log_file /etc/audit/auditd.conf

log_file = /var/log/audit/audit.log
```

Using the path of the directory containing the audit logs, determine if the directory has a mode of "750" or less by using the following command:

```
$ sudo stat -c "%n %a" /var/log/audit

/var/log/audit 750
```

If the audit log directory has a mode more permissive than "750", this is a finding.

Remediation:

Configure the audit log directory to have a mode of "750" or less permissive.
Using the path of the directory containing the audit logs, configure the audit log directory to have a mode of "750" or less permissive by using the following command:

```
$ sudo chmod -R g-w,o-rwx /var/log/audit
```

References:







1. CIS Recommendation "Ensure the audit log file directory mode is configured"

Additional Information:

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CIS Controls:

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

1.130 UBTU-22-653065 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must be configured so that audit configuration files are not write-accessible by unauthorized users.

```
GROUP ID: V-260601
RULE ID: SV-260601r958444
```

Rationale:

Without the capability to restrict which roles and individuals can select which events are audited, unauthorized personnel may be able to prevent the auditing of critical events.

Misconfigured audits may degrade the system's performance by overwhelming the audit log. Misconfigured audits may also make it more difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit:

Verify that `/etc/audit/audit.rules`, `/etc/audit/auditd.conf`, and `/etc/audit/rules.d/*` files have a mode of `"640"` or less permissive by using the following command:

```
$ sudo ls -al /etc/audit/audit.rules /etc/audit/auditd.conf
/etc/audit/rules.d/* | awk '{print $1, $9}'

-rw-r----- /etc/audit/audit.rules
-rw-r----- /etc/audit/auditd.conf
-rw-r----- /etc/audit/rules.d/audit.rules
```

If `/etc/audit/audit.rules`, `/etc/audit/auditd.conf`, or `/etc/audit/rules.d/*` files have a mode more permissive than `"640"`, this is a finding.

Remediation:

Configure `/etc/audit/audit.rules`, `/etc/audit/auditd.conf`, and `/etc/audit/rules.d/*` files to have a mode of `"640"` by using the following command:

```
$ sudo chmod -R 640 /etc/audit/audit.rules /etc/audit/auditd.conf
/etc/audit/rules.d/*
```

References:







1. CIS Recommendation "Ensure audit configuration files mode is configured"

Additional Information:

CCI-000171 Allow organization-defined personnel or roles to select the event types that are to be logged by specific components of the system.

- NIST SP 800-53 :: AU-12 b
- NIST SP 800-53 Revision 4 :: AU-12 b
- NIST SP 800-53 Revision 5 :: AU-12 b
- NIST SP 800-53A :: AU-12.1 (iii)

CIS Controls:

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

1.131 UBTU-22-653070 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must permit only authorized accounts to own the audit configuration files.

```
GROUP ID: V-260602
RULE ID: SV-260602r958444
```

Rationale:

Without the capability to restrict which roles and individuals can select which events are audited, unauthorized personnel may be able to prevent the auditing of critical events.

Misconfigured audits may degrade the system's performance by overwhelming the audit log. Misconfigured audits may also make it more difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit:

Verify that `/etc/audit/audit.rules`, `/etc/audit/auditd.conf`, and `/etc/audit/rules.d/*` files are owned by root account by using the following command:

```
$ sudo ls -al /etc/audit/audit.rules /etc/audit/auditd.conf
/etc/audit/rules.d/* | awk '{print $3, $9}'

root /etc/audit/audit.rules
root /etc/audit/auditd.conf
root /etc/audit/rules.d/audit.rules
```

If `/etc/audit/audit.rules`, `/etc/audit/auditd.conf`, or `/etc/audit/rules.d/*` files are owned by a user other than "root", this is a finding.

Remediation:

Configure `/etc/audit/audit.rules`, `/etc/audit/rules.d/*`, and `/etc/audit/auditd.conf` files to be owned by root by using the following command:

```
$ sudo chown -R root /etc/audit/audit.rules /etc/audit/auditd.conf
/etc/audit/rules.d/*
```

References:







1. CIS Recommendation "Ensure audit configuration files owner is configured"

Additional Information:

CCI-000171 Allow organization-defined personnel or roles to select the event types that are to be logged by specific components of the system.

- NIST SP 800-53 :: AU-12 b
- NIST SP 800-53 Revision 4 :: AU-12 b
- NIST SP 800-53 Revision 5 :: AU-12 b
- NIST SP 800-53A :: AU-12.1 (iii)

CIS Controls:

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

1.132 UBTU-22-653075 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must permit only authorized groups to own the audit configuration files.

```
GROUP ID: V-260603  
RULE ID: SV-260603r958444
```

Rationale:

Without the capability to restrict which roles and individuals can select which events are audited, unauthorized personnel may be able to prevent the auditing of critical events.

Misconfigured audits may degrade the system's performance by overwhelming the audit log. Misconfigured audits may also make it more difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit:

Verify that `/etc/audit/audit.rules`, `/etc/audit/auditd.conf`, and `/etc/audit/rules.d/*` files are owned by root group by using the following command:

```
$ sudo ls -al /etc/audit/audit.rules /etc/audit/auditd.conf  
/etc/audit/rules.d/* | awk '{print $4, $9}'  
  
root /etc/audit/audit.rules  
root /etc/audit/auditd.conf  
root /etc/audit/rules.d/audit.rules
```

If `/etc/audit/audit.rules`, `/etc/audit/auditd.conf`, or `/etc/audit/rules.d/*` files are owned by a group other than "root", this is a finding.

Remediation:

Configure `/etc/audit/audit.rules`, `/etc/audit/rules.d/*`, and `/etc/audit/auditd.conf` files to be owned by root group by using the following command:

```
$ sudo chown -R :root /etc/audit/audit.rules /etc/audit/auditd.conf  
/etc/audit/rules.d/*
```

References:







1. CIS Recommendation "Ensure audit configuration files group owner is configured"

Additional Information:

CCI-000171 Allow organization-defined personnel or roles to select the event types that are to be logged by specific components of the system.

- NIST SP 800-53 :: AU-12 b
- NIST SP 800-53 Revision 4 :: AU-12 b
- NIST SP 800-53 Revision 5 :: AU-12 b
- NIST SP 800-53A :: AU-12.1 (iii)

CIS Controls:

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

1.133 UBTU-22-654010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the `apparmor_parser` command.

```
GROUP ID: V-260604  
RULE ID: SV-260604r958446
```

Rationale:

Audit:

Verify the operating system generates an audit record upon successful/unsuccessful attempts to use the `"apparmor_parser"` command by using the following command:

```
$ sudo auditctl -l | grep apparmor_parser  
  
-a always,exit -S all -F path=/sbin/apparmor_parser -F perm=x -F auid>=1000 -  
F auid!=-1 -F key=perm_chng
```

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

Note: The `"key="` value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the `"apparmor_parser"` command.

Add or modify the following line in the `"/etc/audit/rules.d/stig.rules"` file:

```
-a always,exit -F path=/sbin/apparmor_parser -F perm=x -F auid>=1000 -F  
auid!=unset -k perm_chng
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```





Note: The `"-k "` at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.134 UBTU-22-654015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the `chacl` command.

```
GROUP ID: V-260605  
RULE ID: SV-260605r958446
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the audit system generates an audit record upon successful/unsuccessful attempts to use the "`chacl`" command by using the following command:

```
$ sudo auditctl -l | grep chacl  
  
-a always,exit -S all -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F  
auid!=-1 -F key=perm_chng
```

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

Note: The "`key=`" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "`chacl`" command.

Add or modify the following line in the "`/etc/audit/rules.d/stig.rules`" file:

```
-a always,exit -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F auid!=unset  
-k perm_chng
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "`-k`" at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

References:





1. CIS Recommendation "Ensure successful and unsuccessful attempts to use the chacl command are collected"

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.135 UBTU-22-654020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the chage command.

```
GROUP ID: V-260606
RULE ID: SV-260606r958446
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "chage" command by using the following command:

```
$ sudo auditctl -l | grep -w chage

-a always,exit -S all -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged-chage
```

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

Note: The "key=" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "chage" command.

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-chage
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```





Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.136 UBTU-22-654025 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the chcon command.

```
GROUP ID: V-260607
RULE ID: SV-260607r958446
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the audit system generates an audit record upon successful/unsuccessful attempts to use the "chcon" command by using the following command:

```
$ sudo auditctl -l | grep chcon

-a always,exit -S all -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F
auid!=-1 -F key=perm_chng
```

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

Note: The "key=" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "chcon" command.

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F auid!=unset
-k perm_chng
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

References:





1. CIS Recommendation "Ensure successful and unsuccessful attempts to use the chcon command are collected"

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.137 UBTU-22-654030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the chfn command.

```
GROUP ID: V-260608  
RULE ID: SV-260608r958446
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the audit system generates audit records upon successful/unsuccessful attempts to use the "chfn" command by using the following command:

```
$ sudo auditctl -l | grep /usr/bin/chfn  
  
-a always,exit -S all -F path=/usr/bin/chfn -F perm=x -F auid>=1000 -F  
auid!=-1 -F key=privileged-chfn
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

Note: The "key=" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "chfn" command.

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/chfn -F perm=x -F auid>=1000 -F auid!=unset -  
k privileged-chfn
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```





Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.138 UBTU-22-654035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the chsh command.

```
GROUP ID: V-260609
RULE ID: SV-260609r958446
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

The verify the audit system generates an audit record upon successful/unsuccessful attempts to use the "chsh" command by using the following command:

```
$ sudo auditctl -l | grep chsh

-a always,exit -S all -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F
auid!=-1 -F key=priv_cmd
```

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

Notes: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "chsh" command.

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F auid!=unset -
k priv_cmd
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```





Note: The "-k" at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.139 UBTU-22-654040 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the crontab command.

```
GROUP ID: V-260610  
RULE ID: SV-260610r958446
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "crontab" command by using the following command:

```
$ sudo auditctl -l | grep -w crontab  
  
-a always,exit -S all -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F  
auid!=-1 -F key=privileged-crontab
```

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

Note: The "key=" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "crontab" command.

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-crontab
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```





Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)
-

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>8.5 Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	<u>5.5 Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.140 UBTU-22-654045 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful attempts to use the fdisk command.

```
GROUP ID: V-260611  
RULE ID: SV-260611r991586
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the audit system is configured to audit the execution of the partition management program "fdisk" by using the following command:

```
$ sudo auditctl -l | grep fdisk  
  
-w /usr/sbin/fdisk -p x -k fdisk
```

If the command does not return a line, or the line is commented out, this is a finding.
Note: The "-k" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to audit the execution of the partition management program "fdisk".

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-w /usr/sbin/fdisk -p x -k fdisk
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```





Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.141 UBTU-22-654050 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the gpasswd command.

```
GROUP ID: V-260612  
RULE ID: SV-260612r958446
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "gpasswd" command by using the following command:

```
$ sudo auditctl -l | grep -w gpasswd  
  
-a always,exit -S all -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F  
auid!=-1 -F key=privileged-gpasswd
```

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

Note: The "key=" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "gpasswd" command.

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-gpasswd
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```





Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.142 UBTU-22-654055 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful attempts to use the kmod command.

```
GROUP ID: V-260613
RULE ID: SV-260613r991586
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the operating system is configured to audit the execution of the module management program "kmod" by using the following command:

```
$ sudo auditctl -l | grep kmod

-w /bin/kmod -p x -k module
```

If the command does not return a line, or the line is commented out, this is a finding. Note: The "-k" value is arbitrary and can be different from the example output above.

Remediation:

Configure the operating system to audit the execution of the module management program "kmod".

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-w /bin/kmod -p x -k modules
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

References:





1. CIS Recommendation "Ensure kernel module loading unloading and modification is collected"

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.143 UBTU-22-654060 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful attempts to use modprobe command.

```
GROUP ID: V-260614
RULE ID: SV-260614r991586
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the operating system is configured to audit the execution of the module management program "modprobe" with the following command:

```
$ sudo auditctl -l | grep /sbin/modprobe
-w /sbin/modprobe -p x -k modules
```

If the command does not return a line, or the line is commented out, this is a finding. Note: The "-k" value is arbitrary and can be different from the example output above.

Remediation:

Configure the operating system to audit the execution of the module management program "modprobe".

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-w /sbin/modprobe -p x -k modules
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```





Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.144 UBTU-22-654065 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the mount command.

```
GROUP ID: V-260615  
RULE ID: SV-260615r958446
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the audit system generates audit records upon successful/unsuccessful attempts to use the "mount" command by using the following command:

```
$ sudo auditctl -l | grep /usr/bin/mount  
  
-a always,exit -S all -F path=/usr/bin/mount -F perm=x -F auid>=1000 -F  
auid!=-1 -F key=privileged-mount
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

Note: The "key=" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "mount" command.

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/mount -F perm=x -F auid>=1000 -F auid!=unset  
-k privileged-mount
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

References:





1. CIS Recommendation "Ensure successful file system mounts are collected"

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.145 UBTU-22-654070 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the newgrp command.

```
GROUP ID: V-260616  
RULE ID: SV-260616r958446
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the audit system generates an audit record upon successful/unsuccessful attempts to use the "newgrp" command by using the following command:

```
$ sudo auditctl -l | grep newgrp  
  
-a always,exit -S all -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F  
auid!=-1 -F key=priv_cmd
```

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

Note: The "key=" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "newgrp" command.

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F auid!=unset  
-k priv_cmd
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```





Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.146 UBTU-22-654075 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the `pam_timestamp_check` command.

```
GROUP ID: V-260617
RULE ID: SV-260617r958446
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "pam_timestamp_check" command by using the following command:

```
$ sudo auditctl -l | grep -w pam_timestamp_check

-a always,exit -S all -F path=/usr/sbin/pam_timestamp_check -F perm=x -F
audit>=1000 -F audit!=-1 -F key=privileged-pam_timestamp_check
```

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

Note: The "key=" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "pam_timestamp_check" command.

Add or modify the following line in the `/etc/audit/rules.d/stig.rules` file:

```
-a always,exit -F path=/usr/sbin/pam_timestamp_check -F perm=x -F audit>=1000
-F audit!=unset -k privileged-pam_timestamp_check
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```





Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.147 UBTU-22-654080 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the `passwd` command.

```
GROUP ID: V-260618  
RULE ID: SV-260618r958446
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "passwd" command by using the following command:

```
$ sudo auditctl -l | grep -w passwd  
  
-a always,exit -S all -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F  
auid!=-1 -F key=privileged-passwd
```

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

Note: The "key" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "passwd" command.

Add or modify the following line in the `/etc/audit/rules.d/stig.rules` file:

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

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```





Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.148 UBTU-22-654085 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the setfacl command.

```
GROUP ID: V-260619
RULE ID: SV-260619r958446
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the audit system generates an audit record upon successful/unsuccessful attempts to use the "setfacl" command by using the following command:

```
$ sudo auditctl -l | grep setfacl

-a always,exit -S all -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F
auid!=-1 -F key=perm_chng
```

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

Note: The "key=" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "setfacl" command.

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F
auid!=unset -k perm_chng
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

References:





1. CIS Recommendation "Ensure successful and unsuccessful attempts to use the setfacl command are collected"

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.149 UBTU-22-654090 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the ssh-agent command.

```
GROUP ID: V-260620
RULE ID: SV-260620r958446
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the audit system generates an audit record upon successful/unsuccessful attempts to use the "ssh-agent" command by using the following command:

```
$ sudo auditctl -l | grep /usr/bin/ssh-agent

-a always,exit -S all -F path=/usr/bin/ssh-agent -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged-ssh
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

Note: The "key=" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "ssh-agent" command.

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/ssh-agent -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-ssh
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```





Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.150 UBTU-22-654095 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the ssh-keysign command.

```
GROUP ID: V-260621
RULE ID: SV-260621r958446
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the audit system generates an audit record upon successful/unsuccessful attempts to use the "ssh-keysign" command by using the following command:

```
$ sudo auditctl -l | grep ssh-keysign

-a always,exit -S all -F path=/usr/lib/openssh/ssh-keysign -F perm=x -F
auid>=1000 -F auid!=-1 -F key=privileged-ssh
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

Note: The "key=" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "ssh-keysign" command.

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/lib/openssh/ssh-keysign -F perm=x -F auid>=1000 -
F auid!=unset -k privileged-ssh
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```





Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.151 UBTU-22-654100 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the su command.

```
GROUP ID: V-260622
RULE ID: SV-260622r958446
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the audit system generates audit records upon successful/unsuccessful attempts to use the "su" command by using the following command:

```
$ sudo auditctl -l | grep /bin/su

-a always,exit -S all -F path=/bin/su -F perm=x -F auid>=1000 -F auid!=-1 -F
key=privileged-priv_change
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

Note: The "key=" value is arbitrary and can be different from the example output above.

Remediation:

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

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/bin/su -F perm=x -F auid>=1000 -F auid!=unset -k
privileged-priv_change
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```





Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.152 UBTU-22-654105 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system LTS must generate audit records for successful/unsuccessful uses of the sudo command.

```
GROUP ID: V-260623
RULE ID: SV-260623r958446
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "sudo" command by using the following command:

```
$ sudo auditctl -l | grep /usr/bin/sudo

-a always,exit -S all -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F
auid!=-1 -F key=priv_cmd
```

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

Note: The "key=" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "sudo" command.

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F auid!=unset -
k priv_cmd
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```





Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.153 UBTU-22-654110 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the sudoedit command.

```
GROUP ID: V-260624  
RULE ID: SV-260624r958446
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the audit system generates an audit record upon successful/unsuccessful attempts to use the "sudoedit" command by using the following command:

```
$ sudo auditctl -l | grep /usr/bin/sudoedit  
  
-a always,exit -S all -F path=/usr/bin/sudoedit -F perm=x -F auid>=1000 -F  
auid!=-1 -F key=priv_cmd
```

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

Note: The "key=" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "sudoedit" command.

Add or modify the following line in the "/etc/audit/rules.d/stig.rules":

```
-a always,exit -F path=/usr/bin/sudoedit -F perm=x -F auid>=1000 -F  
auid!=unset -k priv_cmd
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```





Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.154 UBTU-22-654115 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the umount command.

```
GROUP ID: V-260625
RULE ID: SV-260625r958446
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the audit system generates audit records upon successful/unsuccessful attempts to use the "umount" command by using the following command:

```
$ sudo auditctl -l | grep /usr/bin/umount

-a always,exit -S all -F path=/usr/bin/umount -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged-umount
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

Note: The "key=" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "umount" command.

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/umount -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-umount
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

References:





1. CIS Recommendation "Ensure successful file system mounts are collected"

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.155 UBTU-22-654120 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the `unix_update` command.

```
GROUP ID: V-260626  
RULE ID: SV-260626r958446
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "unix_update" command by using the following command:

```
$ sudo auditctl -l | grep -w unix_update  
  
-a always,exit -S all -F path=/sbin/unix_update -F perm=x -F auid>=1000 -F  
auid!=-1 -F key=privileged-unix-update
```

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

Note: The "key=" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "unix_update" command.

Add or modify the following line in the `/etc/audit/rules.d/stig.rules` file:

```
-a always,exit -F path=/sbin/unix_update -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-unix-update
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```





Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.156 UBTU-22-654125 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the usermod command.

```
GROUP ID: V-260627
RULE ID: SV-260627r958446
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "usermod" command by using the following command:

```
$ sudo auditctl -l | grep -w usermod

-a always,exit -S all -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged-usermod
```

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

Note: The "key=" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "usermod" command.

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-usermod
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

References:





1. CIS Recommendation "Ensure successful and unsuccessful attempts to use the usermod command are recorded"

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.157 UBTU-22-654130 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-260628  
RULE ID: SV-260628r958368
```

Rationale:

Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to create an account. Auditing account creation actions provides logging that can be used for forensic purposes.

To address access requirements, many operating systems may be integrated with enterprise level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000476-GPOS-00221

Audit:

Verify the audit system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/group" by using the following command:

```
$ sudo auditctl -l | grep group  
  
-w /etc/group -p wa -k usergroup_modification
```

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

Note: The "-k" value is arbitrary and can be different from the example output above.

Remediation:

Configure the operating system to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/group". Add or modify the following line to "/etc/audit/rules.d/stig.rules":

```
-w /etc/group -p wa -k usergroup_modification
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-001403 Automatically audit account modification actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001404 Automatically audit account disabling actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)





CCI-001405 Automatically audit account removal actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-002130 Automatically audit account enabling actions.

- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.158 UBTU-22-654135 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-260629
RULE ID: SV-260629r958368
```

Rationale:

Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to create an account. Auditing account creation actions provides logging that can be used for forensic purposes.

To address access requirements, many operating systems may be integrated with enterprise level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000476-GPOS-00221

Audit:

Verify the audit system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/gshadow" by using the following command:

```
$ sudo auditctl -l | grep gshadow

-w /etc/gshadow -p wa -k usergroup_modification
```

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

Note: The "-k" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/gshadow". Add or modify the following line to "/etc/audit/rules.d/stig.rules":

```
-w /etc/gshadow -p wa -k usergroup_modification
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-001403 Automatically audit account modification actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001404 Automatically audit account disabling actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)





CCI-001405 Automatically audit account removal actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-002130 Automatically audit account enabling actions.

- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.159 UBTU-22-654140 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-260630
RULE ID: SV-260630r958368
```

Rationale:

Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to create an account. Auditing account creation actions provides logging that can be used for forensic purposes.

To address access requirements, many operating systems may be integrated with enterprise level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000476-GPOS-00221

Audit:

Verify the audit system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/security/opasswd" by using the following command:

```
$ sudo auditctl -l | grep opasswd

-w /etc/security/opasswd -p wa -k usergroup_modification
```

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

Note: The "-k" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/security/opasswd". Add or modify the following line to "/etc/audit/rules.d/stig.rules":

```
-w /etc/security/opasswd -p wa -k usergroup_modification
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-001403 Automatically audit account modification actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001404 Automatically audit account disabling actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)





CCI-001405 Automatically audit account removal actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-002130 Automatically audit account enabling actions.

- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.160 UBTU-22-654145 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-260631  
RULE ID: SV-260631r958368
```

Rationale:

Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to create an account. Auditing account creation actions provides logging that can be used for forensic purposes.

To address access requirements, many operating systems may be integrated with enterprise level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000476-GPOS-00221

Audit:

Verify the audit system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd" by using the following command:

```
$ sudo auditctl -l | grep passwd  
  
-w /etc/passwd -p wa -k usergroup_modification
```

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

Note: The "-k" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd". Add or modify the following line to "/etc/audit/rules.d/stig.rules":

```
-w /etc/passwd -p wa -k usergroup_modification
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-001403 Automatically audit account modification actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001404 Automatically audit account disabling actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)





CCI-001405 Automatically audit account removal actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-002130 Automatically audit account enabling actions.

- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.161 UBTU-22-654150 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-260632  
RULE ID: SV-260632r958368
```

Rationale:

Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to create an account. Auditing account creation actions provides logging that can be used for forensic purposes.

To address access requirements, many operating systems may be integrated with enterprise level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000476-GPOS-00221

Audit:

Verify the audit system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/shadow" by using the following command:

```
$ sudo auditctl -l | grep passwd  
  
-w /etc/shadow -p wa -k usergroup_modification
```

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

Note: The "-k" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/shadow". Add or modify the following line to "/etc/audit/rules.d/stig.rules":

```
-w /etc/shadow -p wa -k usergroup_modification
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-001403 Automatically audit account modification actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001404 Automatically audit account disabling actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001405 Automatically audit account removal actions.





- NIST SP 800-53 :: AC-2 (4)

- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-002130 Automatically audit account enabling actions.

1. NIST SP 800-53 Revision 4 :: AC-2 (4)
2. NIST SP 800-53 Revision 5 :: AC-2 (4)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.162 UBTU-22-654155 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the `chmod`, `fchmod`, and `fchmodat` system calls.

GROUP ID: V-260633 RULE ID: SV-260633r958446

Rationale:

Without generating audit records specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

The system call rules are loaded into a matching engine that intercepts each syscall that all programs on the system makes. Therefore, it is very important to only use syscall rules when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance is helped, though, by combining syscalls into one rule whenever possible.

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206

Audit:

Verify the audit system generates an audit record upon successful/unsuccessful attempts to use the "`chmod`", "`fchmod`", and "`fchmodat`" system calls by using the following command:

```
$ sudo auditctl -l | grep chmod  
  
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=-1  
-F key=perm_chng  
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=-1  
-F key=perm_chng
```

If the command does not return audit rules for the "`chmod`", "`fchmod`" and "`fchmodat`" syscalls or the lines are commented out, this is a finding.

Note: The "`key=`" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "chmod", "fchmod", and "fchmodat" system calls.

Add or modify the following lines in the "/etc/audit/rules.d/stig.rules":

```
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=unset -k perm_chng
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=unset -k perm_chng
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

References:

1. CIS Recommendation "Ensure discretionary access control permission modification events are collected"

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		●	●

1.163 UBTU-22-654160 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the chown, fchown, fchownat, and lchown system calls.

GROUP ID: V-260634 RULE ID: SV-260634r958446

Rationale:

Without generating audit records specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

The system call rules are loaded into a matching engine that intercepts each syscall that all programs on the system makes. Therefore, it is very important to only use syscall rules when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance is helped, though, by combining syscalls into one rule whenever possible.

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206

Audit:

Verify the audit system generates an audit record upon successful/unsuccessful attempts to use the "chown", "fchown", "fchownat", and "lchown" system calls by using the following command:

```
$ sudo auditctl -l | grep chown

-a always,exit -F arch=b32 -S chown,fchown,fchownat,lchown -F auid>=1000 -F auid!=-1 -F key=perm_chng
-a always,exit -F arch=b64 -S chown,fchown,fchownat,lchown -F auid>=1000 -F auid!=-1 -F key=perm_chng
```

If the command does not return audit rules for the "chown", "fchown", "fchownat", and "lchown" syscalls or the lines are commented out, this is a finding.

Note: The "key=" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "chown", "fchown", "fchownat", and "lchown" system calls.

Add or modify the following lines in the "/etc/audit/rules.d/stig.rules":

```
-a always,exit -F arch=b32 -S chown,fchown,fchownat,lchown -F auid>=1000 -F auid!=unset -k perm_chng
-a always,exit -F arch=b64 -S chown,fchown,fchownat,lchown -F auid>=1000 -F auid!=unset -k perm_chng
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

References:

1. CIS Recommendation "Ensure discretionary access control permission modification events are collected"

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		●	●

1.164 UBTU-22-654165 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the creat, open, openat, open_by_handle_at, truncate, and ftruncate system calls.

GROUP ID: V-260635 RULE ID: SV-260635r958446

Rationale:

Without generating audit records specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

The system call rules are loaded into a matching engine that intercepts each syscall that all programs on the system makes. Therefore, it is very important to only use syscall rules when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance is helped, though, by combining syscalls into one rule whenever possible.

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000474-GPOS-00219

Audit:

Verify the audit system generates an audit record upon unsuccessful attempts to use the "creat", "open", "openat", "open_by_handle_at", "truncate", and "ftruncate" system calls by using the following command:

```
$ sudo auditctl -l | grep 'open\|truncate\|creat'

-a always,exit -F arch=b32 -S
creat,open,openat,open_by_handle_at,truncate,ftruncate -F exit=-EPERM -F
auid>=1000 -F auid!=-1 -F key=perm_access
-a always,exit -F arch=b32 -S
creat,open,openat,open_by_handle_at,truncate,ftruncate -F exit=-EACCES -F
auid>=1000 -F auid!=-1 -F key=perm_access
-a always,exit -F arch=b64 -S
creat,open,openat,open_by_handle_at,truncate,ftruncate -F exit=-EPERM -F
auid>=1000 -F auid!=-1 -F key=perm_access
-a always,exit -F arch=b64 -S
creat,open,openat,open_by_handle_at,truncate,ftruncate -F exit=-EACCES -F
auid>=1000 -F auid!=-1 -F key=perm_access
```

If the command does not return audit rules for the "creat", "open", "openat", "open_by_handle_at", "truncate", and "ftruncate" syscalls or the lines are commented out, this is a finding.

Note: The "key=" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any unsuccessful use of the "creat", "open", "openat", "open_by_handle_at", "truncate", and "ftruncate" system calls. Add or modify the following lines in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F arch=b32 -S
creat,open,openat,open_by_handle_at,truncate,ftruncate -F exit=-EPERM -F
auid>=1000 -F auid!=unset -k perm_access
-a always,exit -F arch=b32 -S
creat,open,openat,open_by_handle_at,truncate,ftruncate -F exit=-EACCES -F
auid>=1000 -F auid!=unset -k perm_access
-a always,exit -F arch=b64 -S
creat,open,openat,open_by_handle_at,truncate,ftruncate -F exit=-EPERM -F
auid>=1000 -F auid!=unset -k perm_access
-a always,exit -F arch=b64 -S
creat,open,openat,open_by_handle_at,truncate,ftruncate -F exit=-EACCES -F
auid>=1000 -F auid!=unset -k perm_access
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

References:





1. CIS Recommendation "Ensure unsuccessful file access attempts are collected"

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.165 UBTU-22-654170 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the delete_module system call.

```
GROUP ID: V-260636  
RULE ID: SV-260636r958446
```

Rationale:

Without generating audit records specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000477-GPOS-00222

Audit:

The audit system generates an audit record for any successful/unsuccessful attempts to use the "delete_module" syscall by using the following command:

```
$ sudo auditctl -l | grep -w delete_module  
  
-a always,exit -F arch=b32 -S delete_module -F auid>=1000 -F auid!=-1 -F  
key=module_chng  
-a always,exit -F arch=b64 -S delete_module -F auid>=1000 -F auid!=-1 -F  
key=module_chng
```

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

Note: The "key=" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "delete_module" syscall.

Add or modify the following lines in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F arch=b32 -S delete_module -F auid>=1000 -F auid!=unset -k  
module_chng  
-a always,exit -F arch=b64 -S delete_module -F auid>=1000 -F auid!=unset -k  
module_chng
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

References:





1. CIS Recommendation "Ensure kernel module loading unloading and modification is collected"

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.166 UBTU-22-654175 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for successful/unsuccessful uses of the `init_module` and `finit_module` system calls.

```
GROUP ID: V-260637
RULE ID: SV-260637r958446
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

The system call rules are loaded into a matching engine that intercepts each syscall that all programs on the system makes. Therefore, it is very important to only use syscall rules when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance is helped, though, by combining syscalls into one rule whenever possible.

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000471-GPOS-00216

Audit:

Verify the audit system generates an audit record for any successful/unsuccessful attempts to use the `"init_module"` and `"finit_module"` syscalls by using the following command:

```
$ sudo auditctl -l | grep init_module

-a always,exit -F arch=b32 -S init_module,finit_module -F auid>=1000 -F auid!=-1 -F key=module_chng
-a always,exit -F arch=b64 -S init_module,finit_module -F auid>=1000 -F auid!=-1 -F key=module_chng
```

If the command does not return audit rules for the `"init_module"` and `"finit_module"` syscalls or the lines are commented out, this is a finding.

Note: The `"key="` value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "init_module" and "finit_module" syscalls.

Add or modify the following lines in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F arch=b32 -S init_module,finit_module -F auid>=1000 -F auid!=unset -k module_chng
-a always,exit -F arch=b64 -S init_module,finit_module -F auid>=1000 -F auid!=unset -k module_chng
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

References:





1. CIS Recommendation "Ensure kernel module loading unloading and modification is collected"

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.167 UBTU-22-654180 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for any use of the setxattr, fsetxattr, lsetxattr, removexattr, fremovexattr, and lremovexattr system calls.

GROUP ID: V-260638 RULE ID: SV-260638r958446

Rationale:

Without generating audit records specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

The system call rules are loaded into a matching engine that intercepts each syscall that all programs on the system makes. Therefore, it is very important to only use syscall rules when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance is helped, though, by combining syscalls into one rule whenever possible.

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206

Audit:

Verify the audit system generates an audit record upon successful/unsuccessful attempts to use the "setxattr", "fsetxattr", "lsetxattr", "removexattr", "fremovexattr", and "lremovexattr" system calls by using the following command:

```
$ sudo auditctl -l | grep xattr

-a always,exit -F arch=b32 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F
auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b32 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F auid=0
-k perm_mod
-a always,exit -F arch=b64 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F
auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b64 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F auid=0
-k perm_mod
```

If the command does not return audit rules for the "setxattr", "fsetxattr", "lsetxattr", "removexattr", "fremovexattr" and "lremovexattr" syscalls or the lines are commented out, this is a finding.

Note: The "key=" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "setxattr", "fsetxattr", "lsetxattr", "removexattr", "fremovexattr", and "lremovexattr" system calls.

Add or modify the following lines in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F arch=b32 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F
auid>=1000 -F auid!=unset -k perm_mod
-a always,exit -F arch=b32 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F auid=0
-k perm_mod
-a always,exit -F arch=b64 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F
auid>=1000 -F auid!=unset -k perm_mod
-a always,exit -F arch=b64 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F auid=0
-k perm_mod
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

References:





1. CIS Recommendation "Ensure discretionary access control permission modification events are collected"

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.168 UBTU-22-654185 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for any successful/unsuccessful use of unlink, unlinkat, rename, renameat, and rmdir system calls.

GROUP ID: V-260639 RULE ID: SV-260639r991577

Rationale:

Without generating audit records specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

The system call rules are loaded into a matching engine that intercepts each syscall that all programs on the system makes. Therefore, it is very important to only use syscall rules when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance is helped, though, by combining syscalls into one rule whenever possible.

Audit:

Verify the audit system generates audit records for any successful/unsuccessful use of "unlink", "unlinkat", "rename", "renameat", and "rmdir" system calls by using the following command:

```
$ sudo auditctl -l | grep 'unlink\|rename\|rmdir'

-a always,exit -F arch=b64 -S unlink,unlinkat,rename,renameat,rmdir -F
auid>=1000 -F auid!=-1 -F key=delete
-a always,exit -F arch=b32 -S unlink,unlinkat,rename,renameat,rmdir -F
auid>=1000 -F auid!=-1 -F key=delete
```

If the command does not return audit rules for the "unlink", "unlinkat", "rename", "renameat", and "rmdir" syscalls or the lines are commented out, this is a finding.

Note: The "key" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate audit events for any successful/unsuccessful use of "unlink", "unlinkat", "rename", "renameat", and "rmdir" system calls.

Add or modify the following lines in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F arch=b64 -S unlink,unlinkat,rename,renameat,rmdir -F
auid>=1000 -F auid!=unset -k delete
-a always,exit -F arch=b32 -S unlink,unlinkat,rename,renameat,rmdir -F
auid>=1000 -F auid!=unset -k delete
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

References:





1. CIS Recommendation "Ensure file deletion events by users are collected"

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.169 UBTU-22-654190 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for all events that affect the systemd journal files.

```
GROUP ID: V-260640
RULE ID: SV-260640r991589
```

Rationale:

Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to modify system level binaries and their operation. Auditing the systemd journal files provides logging that can be used for forensic purposes.

To address access requirements, many operating systems may be integrated with enterprise level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Audit:

Verify the audit system generates audit records for all events that affect "/var/log/journal" by using the following command:

```
$ sudo auditctl -l | grep journal
-w /var/log/journal -p wa -k systemd_journal
```

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

Note: The "-k" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate audit records for events that affect "/var/log/journal".

Add or modify the following line to "/etc/audit/rules.d/stig.rules":

```
-w /var/log/journal -p wa -k systemd_journal
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```





Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.170 UBTU-22-654195 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for the /var/log/btmp file.

```
GROUP ID: V-260641
RULE ID: SV-260641r991581
```

Rationale:

Without generating audit records specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the audit system generates audit records showing start and stop times for user access to the system via the "/var/log/btmp" file by using the following command:

```
$ sudo auditctl -l | grep '/var/log/btmp'

-w /var/log/btmp -p wa -k logins
```

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

Note: The "-k" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate audit events showing start and stop times for user access via the "/var/log/btmp" file.

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-w /var/log/btmp -p wa -k logins
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

References:





1. CIS Recommendation "Ensure session initiation information is collected"

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.171 UBTU-22-654200 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for the /var/log/wtmp file.

```
GROUP ID: V-260642
RULE ID: SV-260642r991581
```

Rationale:

Without generating audit records specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the audit system generates audit records showing start and stop times for user access to the system via the "/var/log/wtmp" file by using the following command:

```
$ sudo auditctl -l | grep '/var/log/wtmp'

-w /var/log/wtmp -p wa -k logins
```

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

Note: The "-k" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate audit events showing start and stop times for user access via the "/var/log/wtmp" file.

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-w /var/log/wtmp -p wa -k logins
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.





References:

1. CIS Recommendation "Ensure session initiation information is collected"

Additional Information:

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3. NIST SP 800-53 :: AU-12 c NIST SP 800-53 Revision 4 :: AU-12 c NIST SP 800-53 Revision 5 :: AU-12 c NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.172 UBTU-22-654205 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for the /var/run/utmp file.

```
GROUP ID: V-260643  
RULE ID: SV-260643r991581
```

Rationale:

Without generating audit records specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the audit system generates audit records showing start and stop times for user access to the system via the "/var/run/utmp" file by using the following command:

```
$ sudo auditctl -l | grep '/var/run/utmp'  
  
-w /var/run/utmp -p wa -k logins
```

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

Note: The "-k" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate audit events showing start and stop times for user access via the "/var/run/utmp" file.

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-w /var/run/utmp -p wa -k logins
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

References:





1. CIS Recommendation "Ensure session initiation information is collected"

Additional Information:

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.173 UBTU-22-654210 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for the use and modification of faillog file.

```
GROUP ID: V-260644
RULE ID: SV-260644r958446
```

Rationale:

Without generating audit records specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000470-GPOS-00214, SRG-OS-000473-GPOS-00218

Audit:

Verify the audit system generates an audit record upon successful/unsuccessful modifications to the "faillog" file by using the following command:

```
$ sudo auditctl -l | grep faillog

-w /var/log/faillog -p wa -k logins
```

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

Note: The "-k" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful modifications to the "faillog" file.

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-w /var/log/faillog -p wa -k logins
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```





Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.174 UBTU-22-654215 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for the use and modification of the lastlog file.

```
GROUP ID: V-260645
RULE ID: SV-260645r958446
```

Rationale:

Without generating audit records specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000470-GPOS-00214, SRG-OS-000473-GPOS-00218

Audit:

Verify the audit system generates an audit record when successful/unsuccessful modifications to the "lastlog" file occur by using the following command:

```
$ sudo auditctl -l | grep lastlog

-w /var/log/lastlog -p wa -k login
```

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

Note: The "-k" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful modifications to the "lastlog" file.

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-w /var/log/lastlog -p wa -k logins
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

References:





1. CIS Recommendation "Ensure login and logout events are collected"

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.175 UBTU-22-654220 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records when successful/unsuccessful attempts to modify the /etc/sudoers file occur.

```
GROUP ID: V-260646  
RULE ID: SV-260646r991575
```

Rationale:

Without generating audit records specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the audit system generates audit records for all modifications that affect "/etc/sudoers" by using the following command:

```
$ sudo auditctl -l | grep sudoers  
  
-w /etc/sudoers -p wa -k privilege_modification
```

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

Note: The "-k" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate audit records for all modifications that affect "/etc/sudoers".

Add or modify the following line to "/etc/audit/rules.d/stig.rules":

```
-w /etc/sudoers -p wa -k privilege_modification
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```





Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.176 UBTU-22-654225 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records when successful/unsuccessful attempts to modify the /etc/sudoers.d directory occur.

```
GROUP ID: V-260647  
RULE ID: SV-260647r991575
```

Rationale:

Without generating audit records specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the audit system generates audit records for all modifications that affect "/etc/sudoers.d" directory by using the following command:

```
$ sudo auditctl -l | grep sudoers.d  
  
-w /etc/sudoers.d -p wa -k privilege_modification
```

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

Note: The "-k" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to generate audit records for all modifications that affect "/etc/sudoers.d" directory.

Add or modify the following line to "/etc/audit/rules.d/stig.rules":

```
-w /etc/sudoers.d -p wa -k privilege_modification
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```





Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. he does not need to match the example above.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.177 UBTU-22-654230 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must prevent all software from executing at higher privilege levels than users executing the software and the audit system must be configured to audit the execution of privileged functions.

```
GROUP ID: V-260648
RULE ID: SV-260648r958730
```

Rationale:

In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications/programs, those users are indirectly provided with greater privileges than assigned by the organizations.

Some programs and processes are required to operate at a higher privilege level and therefore should be excluded from the organization-defined software list after review.

Satisfies: SRG-OS-000326-GPOS-00126, SRG-OS-000327-GPOS-00127

Audit:

Verify the audit system audits the execution of privilege functions by auditing the "execve" system call by using the following command:

```
$ sudo auditctl -l | grep execve

-a always,exit -F arch=b64 -S execve -C uid!=euid -F euid=0 -F key=execpriv
-a always,exit -F arch=b64 -S execve -C gid!=egid -F egid=0 -F key=execpriv
-a always,exit -F arch=b32 -S execve -C uid!=euid -F euid=0 -F key=execpriv
-a always,exit -F arch=b32 -S execve -C gid!=egid -F egid=0 -F key=execpriv
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

Note: The "key=" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to audit the execution of all privileged functions.
Add or modify the following lines in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F arch=b64 -S execve -C uid!=euid -F euid=0 -k execpriv
-a always,exit -F arch=b64 -S execve -C gid!=egid -F egid=0 -k execpriv
-a always,exit -F arch=b32 -S execve -C uid!=euid -F euid=0 -k execpriv
-a always,exit -F arch=b32 -S execve -C gid!=egid -F egid=0 -k execpriv
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

References:

1. CIS Recommendation "Ensure actions as another user are always logged"

Additional Information:





CCI-002233 Prevent the organization-defined software from executing at higher privilege levels than users executing the software.

- NIST SP 800-53 Revision 4 :: AC-6 (8)
- NIST SP 800-53 Revision 5 :: AC-6 (8)

CCI-002234 Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.178 UBTU-22-654235 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for privileged activities, nonlocal maintenance, diagnostic sessions and other system-level access.

GROUP ID: V-260649 RULE ID: SV-260649r986298

Rationale:

If events associated with nonlocal administrative access or diagnostic sessions are not logged, a major tool for assessing and investigating attacks would not be available.

This requirement addresses auditing-related issues associated with maintenance tools used specifically for diagnostic and repair actions on organizational information systems.

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection.

This requirement applies to hardware/software diagnostic test equipment or tools. This requirement does not cover hardware/software components that may support information system maintenance, yet are a part of the system, for example, the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch.

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Audit:

Verify the audit system audits activities performed during nonlocal maintenance and diagnostic sessions by using the following command:

<pre>\$ sudo auditctl -l grep sudo.log -w /var/log/sudo.log -p wa -k maintenance</pre>

If the command does not return lines that match the example or the lines are commented out, this is a finding.

Note: The "-k" value is arbitrary and can be different from the example output above.

Remediation:

Configure the audit system to audit activities performed during nonlocal maintenance and diagnostic sessions.

Add or modify the following line in the "/etc/audit/rules.d/stig.rules" file:

```
-w /var/log/sudo.log -p wa -k maintenance
```

To reload the rules file, issue the following command:

```
$ sudo augenrules --load
```

Note: The "-k " at the end of the line gives the rule a unique meaning to help during an audit investigation. The does not need to match the example above.

References:

1. CIS Recommendation "Ensure events that modify the sudo log file are collected"

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)





CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

CCI-004188 Monitor the use of maintenance tools that execute with increased privilege.

- NIST SP 800-53 Revision 5 :: MA-3 (5)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

1.179 UBTU-22-671010 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

The operating system must implement NIST FIPS-validated cryptography to protect classified information and for the following: To provision digital signatures, to generate cryptographic hashes, and to protect unclassified information requiring confidentiality and cryptographic protection in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

GROUP ID: V-260650 RULE ID: SV-260650r987791

Rationale:

Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. The operating system must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Satisfies: SRG-OS-000396-GPOS-00176, SRG-OS-000478-GPOS-00223

Audit:

Verify the system is configured to run in FIPS mode by using the following command:

<pre>\$ grep -i 1 /proc/sys/crypto/fips_enabled 1</pre>

If a value of "1" is not returned, this is a finding.

Remediation:

Configure the operating system to run in FIPS mode. Add "fips=1" to the kernel parameter during the operating system install.

Enabling a FIPS mode on a pre-existing system involves a number of modifications to the operating system. Refer to the Ubuntu Pro security certification documentation for instructions.

A subscription to the "Ubuntu Pro" plan is required to obtain the FIPS Kernel cryptographic modules and enable FIPS.

Note: Ubuntu Pro security certification instructions can be found at:





<https://ubuntu.com/security/certifications/docs/fips-enablement>

Additional Information:

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4 :: SC-13
- NIST SP 800-53 Revision 5 :: SC-13 b

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	STIG RULES		
1.1	UBTU-22-211015 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2	UBTU-22-212010 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.3	UBTU-22-212015 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4	UBTU-22-213010 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5	UBTU-22-213015 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6	UBTU-22-213020 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7	UBTU-22-213025 (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.8	UBTU-22-214010 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.9	UBTU-22-214015 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.10	UBTU-22-215010 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.11	UBTU-22-215015 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.12	UBTU-22-215020 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.13	UBTU-22-215025 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.14	UBTU-22-215030 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.15	UBTU-22-215035 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.16	UBTU-22-231010 (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.17	UBTU-22-232010 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.18	UBTU-22-232015 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.19	UBTU-22-232020 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	UBTU-22-232025 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.21	UBTU-22-232026 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.22	UBTU-22-232027 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.23	UBTU-22-232030 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.24	UBTU-22-232035 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.25	UBTU-22-232040 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.26	UBTU-22-232045 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.27	UBTU-22-232050 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.28	UBTU-22-232055 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.29	UBTU-22-232060 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.30	UBTU-22-232065 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.31	UBTU-22-232070 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.32	UBTU-22-232075 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.33	UBTU-22-232080 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.34	UBTU-22-232085 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.35	UBTU-22-232090 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.36	UBTU-22-232095 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.37	UBTU-22-232100 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.38	UBTU-22-232105 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.39	UBTU-22-232110 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.40	UBTU-22-232120 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.41	UBTU-22-232125 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	UBTU-22-232130 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.43	UBTU-22-232135 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.44	UBTU-22-232140 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.45	UBTU-22-232145 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.46	UBTU-22-251010 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.47	UBTU-22-251015 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.48	UBTU-22-251020 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.49	UBTU-22-251025 (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.50	UBTU-22-251030 (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.51	UBTU-22-252010 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.52	UBTU-22-252015 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.53	UBTU-22-252020 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.54	UBTU-22-253010 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.55	UBTU-22-255010 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.56	UBTU-22-255015 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.57	UBTU-22-255020 (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.58	UBTU-22-255025 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.59	UBTU-22-255030 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.60	UBTU-22-255035 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.61	UBTU-22-255040 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.62	UBTU-22-255045 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.63	UBTU-22-255050 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.64	UBTU-22-255055 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.65	UBTU-22-255060 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.66	UBTU-22-255065 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.67	UBTU-22-271010 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.68	UBTU-22-271015 (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.69	UBTU-22-271020 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.70	UBTU-22-271025 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.71	UBTU-22-271030 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.72	UBTU-22-291010 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.73	UBTU-22-291015 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.74	UBTU-22-411010 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.75	UBTU-22-411015 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.76	UBTU-22-411025 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.77	UBTU-22-411030 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.78	UBTU-22-411035 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.79	UBTU-22-411040 (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.80	UBTU-22-411045 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.81	UBTU-22-412010 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.82	UBTU-22-412020 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.83	UBTU-22-412025 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.84	UBTU-22-412030 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.85	UBTU-22-412035 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.86	UBTU-22-431010 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.87	UBTU-22-431015 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.88	UBTU-22-432010 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.89	UBTU-22-432015 (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.90	UBTU-22-611010 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.91	UBTU-22-611015 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.92	UBTU-22-611020 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.93	UBTU-22-611025 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.94	UBTU-22-611030 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.95	UBTU-22-611035 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.96	UBTU-22-611040 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.97	UBTU-22-611045 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.98	UBTU-22-611055 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.99	UBTU-22-611060 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.100	UBTU-22-611065 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.101	UBTU-22-611070 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.102	UBTU-22-612010 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.103	UBTU-22-612015 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.104	UBTU-22-612020 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.105	UBTU-22-612025 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.106	UBTU-22-612030 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.107	UBTU-22-612035 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.108	UBTU-22-612040 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.109	UBTU-22-631010 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.110	UBTU-22-631015 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.111	UBTU-22-651010 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.112	UBTU-22-651015 (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.113	UBTU-22-651020 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.114	UBTU-22-651025 (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.115	UBTU-22-651030 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.116	UBTU-22-651035 (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.117	UBTU-22-652010 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.118	UBTU-22-652015 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.119	UBTU-22-653010 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.120	UBTU-22-653015 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.121	UBTU-22-653020 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.122	UBTU-22-653025 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.123	UBTU-22-653030 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.124	UBTU-22-653035 (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.125	UBTU-22-653040 (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.126	UBTU-22-653045 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.127	UBTU-22-653050 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.128	UBTU-22-653055 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.129	UBTU-22-653060 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.130	UBTU-22-653065 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.131	UBTU-22-653070 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.132	UBTU-22-653075 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.133	UBTU-22-654010 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.134	UBTU-22-654015 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.135	UBTU-22-654020 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.136	UBTU-22-654025 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.137	UBTU-22-654030 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.138	UBTU-22-654035 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.139	UBTU-22-654040 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.140	UBTU-22-654045 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.141	UBTU-22-654050 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.142	UBTU-22-654055 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.143	UBTU-22-654060 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.144	UBTU-22-654065 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.145	UBTU-22-654070 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.146	UBTU-22-654075 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.147	UBTU-22-654080 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.148	UBTU-22-654085 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.149	UBTU-22-654090 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.150	UBTU-22-654095 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.151	UBTU-22-654100 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.152	UBTU-22-654105 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.153	UBTU-22-654110 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.154	UBTU-22-654115 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.155	UBTU-22-654120 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.156	UBTU-22-654125 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.157	UBTU-22-654130 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.158	UBTU-22-654135 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.159	UBTU-22-654140 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.160	UBTU-22-654145 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.161	UBTU-22-654150 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.162	UBTU-22-654155 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.163	UBTU-22-654160 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.164	UBTU-22-654165 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.165	UBTU-22-654170 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.166	UBTU-22-654175 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.167	UBTU-22-654180 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.168	UBTU-22-654185 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.169	UBTU-22-654190 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.170	UBTU-22-654195 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.171	UBTU-22-654200 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.172	UBTU-22-654205 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.173	UBTU-22-654210 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.174	UBTU-22-654215 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.175	UBTU-22-654220 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.176	UBTU-22-654225 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.177	UBTU-22-654230 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.178	UBTU-22-654235 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.179	UBTU-22-671010 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	UBTU-22-211015	<input type="checkbox"/>	<input type="checkbox"/>
1.8	UBTU-22-214010	<input type="checkbox"/>	<input type="checkbox"/>
1.17	UBTU-22-232010	<input type="checkbox"/>	<input type="checkbox"/>
1.18	UBTU-22-232015	<input type="checkbox"/>	<input type="checkbox"/>
1.19	UBTU-22-232020	<input type="checkbox"/>	<input type="checkbox"/>
1.20	UBTU-22-232025	<input type="checkbox"/>	<input type="checkbox"/>
1.21	UBTU-22-232026	<input type="checkbox"/>	<input type="checkbox"/>
1.22	UBTU-22-232027	<input type="checkbox"/>	<input type="checkbox"/>
1.23	UBTU-22-232030	<input type="checkbox"/>	<input type="checkbox"/>
1.24	UBTU-22-232035	<input type="checkbox"/>	<input type="checkbox"/>
1.25	UBTU-22-232040	<input type="checkbox"/>	<input type="checkbox"/>
1.26	UBTU-22-232045	<input type="checkbox"/>	<input type="checkbox"/>
1.27	UBTU-22-232050	<input type="checkbox"/>	<input type="checkbox"/>
1.28	UBTU-22-232055	<input type="checkbox"/>	<input type="checkbox"/>
1.29	UBTU-22-232060	<input type="checkbox"/>	<input type="checkbox"/>
1.30	UBTU-22-232065	<input type="checkbox"/>	<input type="checkbox"/>
1.31	UBTU-22-232070	<input type="checkbox"/>	<input type="checkbox"/>
1.32	UBTU-22-232075	<input type="checkbox"/>	<input type="checkbox"/>
1.33	UBTU-22-232080	<input type="checkbox"/>	<input type="checkbox"/>
1.34	UBTU-22-232085	<input type="checkbox"/>	<input type="checkbox"/>
1.35	UBTU-22-232090	<input type="checkbox"/>	<input type="checkbox"/>
1.36	UBTU-22-232095	<input type="checkbox"/>	<input type="checkbox"/>
1.37	UBTU-22-232100	<input type="checkbox"/>	<input type="checkbox"/>
1.38	UBTU-22-232105	<input type="checkbox"/>	<input type="checkbox"/>
1.39	UBTU-22-232110	<input type="checkbox"/>	<input type="checkbox"/>
1.40	UBTU-22-232120	<input type="checkbox"/>	<input type="checkbox"/>
1.41	UBTU-22-232125	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.42	UBTU-22-232130	<input type="checkbox"/>	<input type="checkbox"/>
1.43	UBTU-22-232135	<input type="checkbox"/>	<input type="checkbox"/>
1.44	UBTU-22-232140	<input type="checkbox"/>	<input type="checkbox"/>
1.45	UBTU-22-232145	<input type="checkbox"/>	<input type="checkbox"/>
1.46	UBTU-22-251010	<input type="checkbox"/>	<input type="checkbox"/>
1.47	UBTU-22-251015	<input type="checkbox"/>	<input type="checkbox"/>
1.48	UBTU-22-251020	<input type="checkbox"/>	<input type="checkbox"/>
1.49	UBTU-22-251025	<input type="checkbox"/>	<input type="checkbox"/>
1.50	UBTU-22-251030	<input type="checkbox"/>	<input type="checkbox"/>
1.57	UBTU-22-255020	<input type="checkbox"/>	<input type="checkbox"/>
1.67	UBTU-22-271010	<input type="checkbox"/>	<input type="checkbox"/>
1.68	UBTU-22-271015	<input type="checkbox"/>	<input type="checkbox"/>
1.70	UBTU-22-271025	<input type="checkbox"/>	<input type="checkbox"/>
1.71	UBTU-22-271030	<input type="checkbox"/>	<input type="checkbox"/>
1.74	UBTU-22-411010	<input type="checkbox"/>	<input type="checkbox"/>
1.81	UBTU-22-412010	<input type="checkbox"/>	<input type="checkbox"/>
1.82	UBTU-22-412020	<input type="checkbox"/>	<input type="checkbox"/>
1.83	UBTU-22-412025	<input type="checkbox"/>	<input type="checkbox"/>
1.84	UBTU-22-412030	<input type="checkbox"/>	<input type="checkbox"/>
1.85	UBTU-22-412035	<input type="checkbox"/>	<input type="checkbox"/>
1.86	UBTU-22-431010	<input type="checkbox"/>	<input type="checkbox"/>
1.88	UBTU-22-432010	<input type="checkbox"/>	<input type="checkbox"/>
1.89	UBTU-22-432015	<input type="checkbox"/>	<input type="checkbox"/>
1.109	UBTU-22-631010	<input type="checkbox"/>	<input type="checkbox"/>
1.110	UBTU-22-631015	<input type="checkbox"/>	<input type="checkbox"/>
1.114	UBTU-22-651025	<input type="checkbox"/>	<input type="checkbox"/>
1.117	UBTU-22-652010	<input type="checkbox"/>	<input type="checkbox"/>
1.118	UBTU-22-652015	<input type="checkbox"/>	<input type="checkbox"/>
1.119	UBTU-22-653010	<input type="checkbox"/>	<input type="checkbox"/>
1.120	UBTU-22-653015	<input type="checkbox"/>	<input type="checkbox"/>
1.121	UBTU-22-653020	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.126	UBTU-22-653045	<input type="checkbox"/>	<input type="checkbox"/>
1.127	UBTU-22-653050	<input type="checkbox"/>	<input type="checkbox"/>
1.128	UBTU-22-653055	<input type="checkbox"/>	<input type="checkbox"/>
1.129	UBTU-22-653060	<input type="checkbox"/>	<input type="checkbox"/>
1.130	UBTU-22-653065	<input type="checkbox"/>	<input type="checkbox"/>
1.131	UBTU-22-653070	<input type="checkbox"/>	<input type="checkbox"/>
1.132	UBTU-22-653075	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	UBTU-22-211015	<input type="checkbox"/>	<input type="checkbox"/>
1.2	UBTU-22-212010	<input type="checkbox"/>	<input type="checkbox"/>
1.4	UBTU-22-213010	<input type="checkbox"/>	<input type="checkbox"/>
1.5	UBTU-22-213015	<input type="checkbox"/>	<input type="checkbox"/>
1.6	UBTU-22-213020	<input type="checkbox"/>	<input type="checkbox"/>
1.7	UBTU-22-213025	<input type="checkbox"/>	<input type="checkbox"/>
1.8	UBTU-22-214010	<input type="checkbox"/>	<input type="checkbox"/>
1.11	UBTU-22-215015	<input type="checkbox"/>	<input type="checkbox"/>
1.12	UBTU-22-215020	<input type="checkbox"/>	<input type="checkbox"/>
1.13	UBTU-22-215025	<input type="checkbox"/>	<input type="checkbox"/>
1.14	UBTU-22-215030	<input type="checkbox"/>	<input type="checkbox"/>
1.15	UBTU-22-215035	<input type="checkbox"/>	<input type="checkbox"/>
1.17	UBTU-22-232010	<input type="checkbox"/>	<input type="checkbox"/>
1.18	UBTU-22-232015	<input type="checkbox"/>	<input type="checkbox"/>
1.19	UBTU-22-232020	<input type="checkbox"/>	<input type="checkbox"/>
1.20	UBTU-22-232025	<input type="checkbox"/>	<input type="checkbox"/>
1.21	UBTU-22-232026	<input type="checkbox"/>	<input type="checkbox"/>
1.22	UBTU-22-232027	<input type="checkbox"/>	<input type="checkbox"/>
1.23	UBTU-22-232030	<input type="checkbox"/>	<input type="checkbox"/>
1.24	UBTU-22-232035	<input type="checkbox"/>	<input type="checkbox"/>
1.25	UBTU-22-232040	<input type="checkbox"/>	<input type="checkbox"/>
1.26	UBTU-22-232045	<input type="checkbox"/>	<input type="checkbox"/>
1.27	UBTU-22-232050	<input type="checkbox"/>	<input type="checkbox"/>
1.28	UBTU-22-232055	<input type="checkbox"/>	<input type="checkbox"/>
1.29	UBTU-22-232060	<input type="checkbox"/>	<input type="checkbox"/>
1.30	UBTU-22-232065	<input type="checkbox"/>	<input type="checkbox"/>
1.31	UBTU-22-232070	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.32	UBTU-22-232075	<input type="checkbox"/>	<input type="checkbox"/>
1.33	UBTU-22-232080	<input type="checkbox"/>	<input type="checkbox"/>
1.34	UBTU-22-232085	<input type="checkbox"/>	<input type="checkbox"/>
1.35	UBTU-22-232090	<input type="checkbox"/>	<input type="checkbox"/>
1.36	UBTU-22-232095	<input type="checkbox"/>	<input type="checkbox"/>
1.37	UBTU-22-232100	<input type="checkbox"/>	<input type="checkbox"/>
1.38	UBTU-22-232105	<input type="checkbox"/>	<input type="checkbox"/>
1.39	UBTU-22-232110	<input type="checkbox"/>	<input type="checkbox"/>
1.40	UBTU-22-232120	<input type="checkbox"/>	<input type="checkbox"/>
1.41	UBTU-22-232125	<input type="checkbox"/>	<input type="checkbox"/>
1.42	UBTU-22-232130	<input type="checkbox"/>	<input type="checkbox"/>
1.43	UBTU-22-232135	<input type="checkbox"/>	<input type="checkbox"/>
1.44	UBTU-22-232140	<input type="checkbox"/>	<input type="checkbox"/>
1.45	UBTU-22-232145	<input type="checkbox"/>	<input type="checkbox"/>
1.46	UBTU-22-251010	<input type="checkbox"/>	<input type="checkbox"/>
1.47	UBTU-22-251015	<input type="checkbox"/>	<input type="checkbox"/>
1.48	UBTU-22-251020	<input type="checkbox"/>	<input type="checkbox"/>
1.49	UBTU-22-251025	<input type="checkbox"/>	<input type="checkbox"/>
1.50	UBTU-22-251030	<input type="checkbox"/>	<input type="checkbox"/>
1.51	UBTU-22-252010	<input type="checkbox"/>	<input type="checkbox"/>
1.52	UBTU-22-252015	<input type="checkbox"/>	<input type="checkbox"/>
1.53	UBTU-22-252020	<input type="checkbox"/>	<input type="checkbox"/>
1.54	UBTU-22-253010	<input type="checkbox"/>	<input type="checkbox"/>
1.55	UBTU-22-255010	<input type="checkbox"/>	<input type="checkbox"/>
1.56	UBTU-22-255015	<input type="checkbox"/>	<input type="checkbox"/>
1.57	UBTU-22-255020	<input type="checkbox"/>	<input type="checkbox"/>
1.58	UBTU-22-255025	<input type="checkbox"/>	<input type="checkbox"/>
1.61	UBTU-22-255040	<input type="checkbox"/>	<input type="checkbox"/>
1.62	UBTU-22-255045	<input type="checkbox"/>	<input type="checkbox"/>
1.63	UBTU-22-255050	<input type="checkbox"/>	<input type="checkbox"/>
1.64	UBTU-22-255055	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.65	UBTU-22-255060	<input type="checkbox"/>	<input type="checkbox"/>
1.66	UBTU-22-255065	<input type="checkbox"/>	<input type="checkbox"/>
1.67	UBTU-22-271010	<input type="checkbox"/>	<input type="checkbox"/>
1.68	UBTU-22-271015	<input type="checkbox"/>	<input type="checkbox"/>
1.70	UBTU-22-271025	<input type="checkbox"/>	<input type="checkbox"/>
1.71	UBTU-22-271030	<input type="checkbox"/>	<input type="checkbox"/>
1.72	UBTU-22-291010	<input type="checkbox"/>	<input type="checkbox"/>
1.74	UBTU-22-411010	<input type="checkbox"/>	<input type="checkbox"/>
1.76	UBTU-22-411025	<input type="checkbox"/>	<input type="checkbox"/>
1.77	UBTU-22-411030	<input type="checkbox"/>	<input type="checkbox"/>
1.78	UBTU-22-411035	<input type="checkbox"/>	<input type="checkbox"/>
1.79	UBTU-22-411040	<input type="checkbox"/>	<input type="checkbox"/>
1.80	UBTU-22-411045	<input type="checkbox"/>	<input type="checkbox"/>
1.81	UBTU-22-412010	<input type="checkbox"/>	<input type="checkbox"/>
1.82	UBTU-22-412020	<input type="checkbox"/>	<input type="checkbox"/>
1.83	UBTU-22-412025	<input type="checkbox"/>	<input type="checkbox"/>
1.84	UBTU-22-412030	<input type="checkbox"/>	<input type="checkbox"/>
1.85	UBTU-22-412035	<input type="checkbox"/>	<input type="checkbox"/>
1.86	UBTU-22-431010	<input type="checkbox"/>	<input type="checkbox"/>
1.88	UBTU-22-432010	<input type="checkbox"/>	<input type="checkbox"/>
1.89	UBTU-22-432015	<input type="checkbox"/>	<input type="checkbox"/>
1.90	UBTU-22-611010	<input type="checkbox"/>	<input type="checkbox"/>
1.91	UBTU-22-611015	<input type="checkbox"/>	<input type="checkbox"/>
1.92	UBTU-22-611020	<input type="checkbox"/>	<input type="checkbox"/>
1.93	UBTU-22-611025	<input type="checkbox"/>	<input type="checkbox"/>
1.94	UBTU-22-611030	<input type="checkbox"/>	<input type="checkbox"/>
1.95	UBTU-22-611035	<input type="checkbox"/>	<input type="checkbox"/>
1.96	UBTU-22-611040	<input type="checkbox"/>	<input type="checkbox"/>
1.97	UBTU-22-611045	<input type="checkbox"/>	<input type="checkbox"/>
1.98	UBTU-22-611055	<input type="checkbox"/>	<input type="checkbox"/>
1.99	UBTU-22-611060	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.100	UBTU-22-611065	<input type="checkbox"/>	<input type="checkbox"/>
1.101	UBTU-22-611070	<input type="checkbox"/>	<input type="checkbox"/>
1.102	UBTU-22-612010	<input type="checkbox"/>	<input type="checkbox"/>
1.103	UBTU-22-612015	<input type="checkbox"/>	<input type="checkbox"/>
1.104	UBTU-22-612020	<input type="checkbox"/>	<input type="checkbox"/>
1.105	UBTU-22-612025	<input type="checkbox"/>	<input type="checkbox"/>
1.106	UBTU-22-612030	<input type="checkbox"/>	<input type="checkbox"/>
1.107	UBTU-22-612035	<input type="checkbox"/>	<input type="checkbox"/>
1.108	UBTU-22-612040	<input type="checkbox"/>	<input type="checkbox"/>
1.109	UBTU-22-631010	<input type="checkbox"/>	<input type="checkbox"/>
1.110	UBTU-22-631015	<input type="checkbox"/>	<input type="checkbox"/>
1.114	UBTU-22-651025	<input type="checkbox"/>	<input type="checkbox"/>
1.116	UBTU-22-651035	<input type="checkbox"/>	<input type="checkbox"/>
1.117	UBTU-22-652010	<input type="checkbox"/>	<input type="checkbox"/>
1.118	UBTU-22-652015	<input type="checkbox"/>	<input type="checkbox"/>
1.119	UBTU-22-653010	<input type="checkbox"/>	<input type="checkbox"/>
1.120	UBTU-22-653015	<input type="checkbox"/>	<input type="checkbox"/>
1.121	UBTU-22-653020	<input type="checkbox"/>	<input type="checkbox"/>
1.122	UBTU-22-653025	<input type="checkbox"/>	<input type="checkbox"/>
1.123	UBTU-22-653030	<input type="checkbox"/>	<input type="checkbox"/>
1.124	UBTU-22-653035	<input type="checkbox"/>	<input type="checkbox"/>
1.125	UBTU-22-653040	<input type="checkbox"/>	<input type="checkbox"/>
1.126	UBTU-22-653045	<input type="checkbox"/>	<input type="checkbox"/>
1.127	UBTU-22-653050	<input type="checkbox"/>	<input type="checkbox"/>
1.128	UBTU-22-653055	<input type="checkbox"/>	<input type="checkbox"/>
1.129	UBTU-22-653060	<input type="checkbox"/>	<input type="checkbox"/>
1.130	UBTU-22-653065	<input type="checkbox"/>	<input type="checkbox"/>
1.131	UBTU-22-653070	<input type="checkbox"/>	<input type="checkbox"/>
1.132	UBTU-22-653075	<input type="checkbox"/>	<input type="checkbox"/>
1.133	UBTU-22-654010	<input type="checkbox"/>	<input type="checkbox"/>
1.134	UBTU-22-654015	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.135	UBTU-22-654020	<input type="checkbox"/>	<input type="checkbox"/>
1.136	UBTU-22-654025	<input type="checkbox"/>	<input type="checkbox"/>
1.137	UBTU-22-654030	<input type="checkbox"/>	<input type="checkbox"/>
1.138	UBTU-22-654035	<input type="checkbox"/>	<input type="checkbox"/>
1.139	UBTU-22-654040	<input type="checkbox"/>	<input type="checkbox"/>
1.140	UBTU-22-654045	<input type="checkbox"/>	<input type="checkbox"/>
1.141	UBTU-22-654050	<input type="checkbox"/>	<input type="checkbox"/>
1.142	UBTU-22-654055	<input type="checkbox"/>	<input type="checkbox"/>
1.143	UBTU-22-654060	<input type="checkbox"/>	<input type="checkbox"/>
1.144	UBTU-22-654065	<input type="checkbox"/>	<input type="checkbox"/>
1.145	UBTU-22-654070	<input type="checkbox"/>	<input type="checkbox"/>
1.146	UBTU-22-654075	<input type="checkbox"/>	<input type="checkbox"/>
1.147	UBTU-22-654080	<input type="checkbox"/>	<input type="checkbox"/>
1.148	UBTU-22-654085	<input type="checkbox"/>	<input type="checkbox"/>
1.149	UBTU-22-654090	<input type="checkbox"/>	<input type="checkbox"/>
1.150	UBTU-22-654095	<input type="checkbox"/>	<input type="checkbox"/>
1.151	UBTU-22-654100	<input type="checkbox"/>	<input type="checkbox"/>
1.152	UBTU-22-654105	<input type="checkbox"/>	<input type="checkbox"/>
1.153	UBTU-22-654110	<input type="checkbox"/>	<input type="checkbox"/>
1.154	UBTU-22-654115	<input type="checkbox"/>	<input type="checkbox"/>
1.155	UBTU-22-654120	<input type="checkbox"/>	<input type="checkbox"/>
1.156	UBTU-22-654125	<input type="checkbox"/>	<input type="checkbox"/>
1.157	UBTU-22-654130	<input type="checkbox"/>	<input type="checkbox"/>
1.158	UBTU-22-654135	<input type="checkbox"/>	<input type="checkbox"/>
1.159	UBTU-22-654140	<input type="checkbox"/>	<input type="checkbox"/>
1.160	UBTU-22-654145	<input type="checkbox"/>	<input type="checkbox"/>
1.161	UBTU-22-654150	<input type="checkbox"/>	<input type="checkbox"/>
1.162	UBTU-22-654155	<input type="checkbox"/>	<input type="checkbox"/>
1.163	UBTU-22-654160	<input type="checkbox"/>	<input type="checkbox"/>
1.164	UBTU-22-654165	<input type="checkbox"/>	<input type="checkbox"/>
1.165	UBTU-22-654170	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.166	UBTU-22-654175	<input type="checkbox"/>	<input type="checkbox"/>
1.167	UBTU-22-654180	<input type="checkbox"/>	<input type="checkbox"/>
1.168	UBTU-22-654185	<input type="checkbox"/>	<input type="checkbox"/>
1.169	UBTU-22-654190	<input type="checkbox"/>	<input type="checkbox"/>
1.170	UBTU-22-654195	<input type="checkbox"/>	<input type="checkbox"/>
1.171	UBTU-22-654200	<input type="checkbox"/>	<input type="checkbox"/>
1.172	UBTU-22-654205	<input type="checkbox"/>	<input type="checkbox"/>
1.173	UBTU-22-654210	<input type="checkbox"/>	<input type="checkbox"/>
1.174	UBTU-22-654215	<input type="checkbox"/>	<input type="checkbox"/>
1.175	UBTU-22-654220	<input type="checkbox"/>	<input type="checkbox"/>
1.176	UBTU-22-654225	<input type="checkbox"/>	<input type="checkbox"/>
1.177	UBTU-22-654230	<input type="checkbox"/>	<input type="checkbox"/>
1.178	UBTU-22-654235	<input type="checkbox"/>	<input type="checkbox"/>
1.179	UBTU-22-671010	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	UBTU-22-211015	<input type="checkbox"/>	<input type="checkbox"/>
1.2	UBTU-22-212010	<input type="checkbox"/>	<input type="checkbox"/>
1.4	UBTU-22-213010	<input type="checkbox"/>	<input type="checkbox"/>
1.5	UBTU-22-213015	<input type="checkbox"/>	<input type="checkbox"/>
1.6	UBTU-22-213020	<input type="checkbox"/>	<input type="checkbox"/>
1.7	UBTU-22-213025	<input type="checkbox"/>	<input type="checkbox"/>
1.8	UBTU-22-214010	<input type="checkbox"/>	<input type="checkbox"/>
1.11	UBTU-22-215015	<input type="checkbox"/>	<input type="checkbox"/>
1.12	UBTU-22-215020	<input type="checkbox"/>	<input type="checkbox"/>
1.13	UBTU-22-215025	<input type="checkbox"/>	<input type="checkbox"/>
1.14	UBTU-22-215030	<input type="checkbox"/>	<input type="checkbox"/>
1.15	UBTU-22-215035	<input type="checkbox"/>	<input type="checkbox"/>
1.16	UBTU-22-231010	<input type="checkbox"/>	<input type="checkbox"/>
1.17	UBTU-22-232010	<input type="checkbox"/>	<input type="checkbox"/>
1.18	UBTU-22-232015	<input type="checkbox"/>	<input type="checkbox"/>
1.19	UBTU-22-232020	<input type="checkbox"/>	<input type="checkbox"/>
1.20	UBTU-22-232025	<input type="checkbox"/>	<input type="checkbox"/>
1.21	UBTU-22-232026	<input type="checkbox"/>	<input type="checkbox"/>
1.22	UBTU-22-232027	<input type="checkbox"/>	<input type="checkbox"/>
1.23	UBTU-22-232030	<input type="checkbox"/>	<input type="checkbox"/>
1.24	UBTU-22-232035	<input type="checkbox"/>	<input type="checkbox"/>
1.25	UBTU-22-232040	<input type="checkbox"/>	<input type="checkbox"/>
1.26	UBTU-22-232045	<input type="checkbox"/>	<input type="checkbox"/>
1.27	UBTU-22-232050	<input type="checkbox"/>	<input type="checkbox"/>
1.28	UBTU-22-232055	<input type="checkbox"/>	<input type="checkbox"/>
1.29	UBTU-22-232060	<input type="checkbox"/>	<input type="checkbox"/>
1.30	UBTU-22-232065	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.31	UBTU-22-232070	<input type="checkbox"/>	<input type="checkbox"/>
1.32	UBTU-22-232075	<input type="checkbox"/>	<input type="checkbox"/>
1.33	UBTU-22-232080	<input type="checkbox"/>	<input type="checkbox"/>
1.34	UBTU-22-232085	<input type="checkbox"/>	<input type="checkbox"/>
1.35	UBTU-22-232090	<input type="checkbox"/>	<input type="checkbox"/>
1.36	UBTU-22-232095	<input type="checkbox"/>	<input type="checkbox"/>
1.37	UBTU-22-232100	<input type="checkbox"/>	<input type="checkbox"/>
1.38	UBTU-22-232105	<input type="checkbox"/>	<input type="checkbox"/>
1.39	UBTU-22-232110	<input type="checkbox"/>	<input type="checkbox"/>
1.40	UBTU-22-232120	<input type="checkbox"/>	<input type="checkbox"/>
1.41	UBTU-22-232125	<input type="checkbox"/>	<input type="checkbox"/>
1.42	UBTU-22-232130	<input type="checkbox"/>	<input type="checkbox"/>
1.43	UBTU-22-232135	<input type="checkbox"/>	<input type="checkbox"/>
1.44	UBTU-22-232140	<input type="checkbox"/>	<input type="checkbox"/>
1.45	UBTU-22-232145	<input type="checkbox"/>	<input type="checkbox"/>
1.46	UBTU-22-251010	<input type="checkbox"/>	<input type="checkbox"/>
1.47	UBTU-22-251015	<input type="checkbox"/>	<input type="checkbox"/>
1.48	UBTU-22-251020	<input type="checkbox"/>	<input type="checkbox"/>
1.49	UBTU-22-251025	<input type="checkbox"/>	<input type="checkbox"/>
1.50	UBTU-22-251030	<input type="checkbox"/>	<input type="checkbox"/>
1.51	UBTU-22-252010	<input type="checkbox"/>	<input type="checkbox"/>
1.52	UBTU-22-252015	<input type="checkbox"/>	<input type="checkbox"/>
1.53	UBTU-22-252020	<input type="checkbox"/>	<input type="checkbox"/>
1.54	UBTU-22-253010	<input type="checkbox"/>	<input type="checkbox"/>
1.55	UBTU-22-255010	<input type="checkbox"/>	<input type="checkbox"/>
1.56	UBTU-22-255015	<input type="checkbox"/>	<input type="checkbox"/>
1.57	UBTU-22-255020	<input type="checkbox"/>	<input type="checkbox"/>
1.58	UBTU-22-255025	<input type="checkbox"/>	<input type="checkbox"/>
1.61	UBTU-22-255040	<input type="checkbox"/>	<input type="checkbox"/>
1.62	UBTU-22-255045	<input type="checkbox"/>	<input type="checkbox"/>
1.63	UBTU-22-255050	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.64	UBTU-22-255055	<input type="checkbox"/>	<input type="checkbox"/>
1.65	UBTU-22-255060	<input type="checkbox"/>	<input type="checkbox"/>
1.66	UBTU-22-255065	<input type="checkbox"/>	<input type="checkbox"/>
1.67	UBTU-22-271010	<input type="checkbox"/>	<input type="checkbox"/>
1.68	UBTU-22-271015	<input type="checkbox"/>	<input type="checkbox"/>
1.70	UBTU-22-271025	<input type="checkbox"/>	<input type="checkbox"/>
1.71	UBTU-22-271030	<input type="checkbox"/>	<input type="checkbox"/>
1.72	UBTU-22-291010	<input type="checkbox"/>	<input type="checkbox"/>
1.73	UBTU-22-291015	<input type="checkbox"/>	<input type="checkbox"/>
1.74	UBTU-22-411010	<input type="checkbox"/>	<input type="checkbox"/>
1.76	UBTU-22-411025	<input type="checkbox"/>	<input type="checkbox"/>
1.77	UBTU-22-411030	<input type="checkbox"/>	<input type="checkbox"/>
1.78	UBTU-22-411035	<input type="checkbox"/>	<input type="checkbox"/>
1.79	UBTU-22-411040	<input type="checkbox"/>	<input type="checkbox"/>
1.80	UBTU-22-411045	<input type="checkbox"/>	<input type="checkbox"/>
1.81	UBTU-22-412010	<input type="checkbox"/>	<input type="checkbox"/>
1.82	UBTU-22-412020	<input type="checkbox"/>	<input type="checkbox"/>
1.83	UBTU-22-412025	<input type="checkbox"/>	<input type="checkbox"/>
1.84	UBTU-22-412030	<input type="checkbox"/>	<input type="checkbox"/>
1.85	UBTU-22-412035	<input type="checkbox"/>	<input type="checkbox"/>
1.86	UBTU-22-431010	<input type="checkbox"/>	<input type="checkbox"/>
1.87	UBTU-22-431015	<input type="checkbox"/>	<input type="checkbox"/>
1.88	UBTU-22-432010	<input type="checkbox"/>	<input type="checkbox"/>
1.89	UBTU-22-432015	<input type="checkbox"/>	<input type="checkbox"/>
1.90	UBTU-22-611010	<input type="checkbox"/>	<input type="checkbox"/>
1.91	UBTU-22-611015	<input type="checkbox"/>	<input type="checkbox"/>
1.92	UBTU-22-611020	<input type="checkbox"/>	<input type="checkbox"/>
1.93	UBTU-22-611025	<input type="checkbox"/>	<input type="checkbox"/>
1.94	UBTU-22-611030	<input type="checkbox"/>	<input type="checkbox"/>
1.95	UBTU-22-611035	<input type="checkbox"/>	<input type="checkbox"/>
1.96	UBTU-22-611040	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.97	UBTU-22-611045	<input type="checkbox"/>	<input type="checkbox"/>
1.98	UBTU-22-611055	<input type="checkbox"/>	<input type="checkbox"/>
1.99	UBTU-22-611060	<input type="checkbox"/>	<input type="checkbox"/>
1.100	UBTU-22-611065	<input type="checkbox"/>	<input type="checkbox"/>
1.101	UBTU-22-611070	<input type="checkbox"/>	<input type="checkbox"/>
1.102	UBTU-22-612010	<input type="checkbox"/>	<input type="checkbox"/>
1.103	UBTU-22-612015	<input type="checkbox"/>	<input type="checkbox"/>
1.104	UBTU-22-612020	<input type="checkbox"/>	<input type="checkbox"/>
1.105	UBTU-22-612025	<input type="checkbox"/>	<input type="checkbox"/>
1.106	UBTU-22-612030	<input type="checkbox"/>	<input type="checkbox"/>
1.107	UBTU-22-612035	<input type="checkbox"/>	<input type="checkbox"/>
1.108	UBTU-22-612040	<input type="checkbox"/>	<input type="checkbox"/>
1.109	UBTU-22-631010	<input type="checkbox"/>	<input type="checkbox"/>
1.110	UBTU-22-631015	<input type="checkbox"/>	<input type="checkbox"/>
1.111	UBTU-22-651010	<input type="checkbox"/>	<input type="checkbox"/>
1.112	UBTU-22-651015	<input type="checkbox"/>	<input type="checkbox"/>
1.113	UBTU-22-651020	<input type="checkbox"/>	<input type="checkbox"/>
1.114	UBTU-22-651025	<input type="checkbox"/>	<input type="checkbox"/>
1.116	UBTU-22-651035	<input type="checkbox"/>	<input type="checkbox"/>
1.117	UBTU-22-652010	<input type="checkbox"/>	<input type="checkbox"/>
1.118	UBTU-22-652015	<input type="checkbox"/>	<input type="checkbox"/>
1.119	UBTU-22-653010	<input type="checkbox"/>	<input type="checkbox"/>
1.120	UBTU-22-653015	<input type="checkbox"/>	<input type="checkbox"/>
1.121	UBTU-22-653020	<input type="checkbox"/>	<input type="checkbox"/>
1.122	UBTU-22-653025	<input type="checkbox"/>	<input type="checkbox"/>
1.123	UBTU-22-653030	<input type="checkbox"/>	<input type="checkbox"/>
1.124	UBTU-22-653035	<input type="checkbox"/>	<input type="checkbox"/>
1.125	UBTU-22-653040	<input type="checkbox"/>	<input type="checkbox"/>
1.126	UBTU-22-653045	<input type="checkbox"/>	<input type="checkbox"/>
1.127	UBTU-22-653050	<input type="checkbox"/>	<input type="checkbox"/>
1.128	UBTU-22-653055	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.129	UBTU-22-653060	<input type="checkbox"/>	<input type="checkbox"/>
1.130	UBTU-22-653065	<input type="checkbox"/>	<input type="checkbox"/>
1.131	UBTU-22-653070	<input type="checkbox"/>	<input type="checkbox"/>
1.132	UBTU-22-653075	<input type="checkbox"/>	<input type="checkbox"/>
1.133	UBTU-22-654010	<input type="checkbox"/>	<input type="checkbox"/>
1.134	UBTU-22-654015	<input type="checkbox"/>	<input type="checkbox"/>
1.135	UBTU-22-654020	<input type="checkbox"/>	<input type="checkbox"/>
1.136	UBTU-22-654025	<input type="checkbox"/>	<input type="checkbox"/>
1.137	UBTU-22-654030	<input type="checkbox"/>	<input type="checkbox"/>
1.138	UBTU-22-654035	<input type="checkbox"/>	<input type="checkbox"/>
1.139	UBTU-22-654040	<input type="checkbox"/>	<input type="checkbox"/>
1.140	UBTU-22-654045	<input type="checkbox"/>	<input type="checkbox"/>
1.141	UBTU-22-654050	<input type="checkbox"/>	<input type="checkbox"/>
1.142	UBTU-22-654055	<input type="checkbox"/>	<input type="checkbox"/>
1.143	UBTU-22-654060	<input type="checkbox"/>	<input type="checkbox"/>
1.144	UBTU-22-654065	<input type="checkbox"/>	<input type="checkbox"/>
1.145	UBTU-22-654070	<input type="checkbox"/>	<input type="checkbox"/>
1.146	UBTU-22-654075	<input type="checkbox"/>	<input type="checkbox"/>
1.147	UBTU-22-654080	<input type="checkbox"/>	<input type="checkbox"/>
1.148	UBTU-22-654085	<input type="checkbox"/>	<input type="checkbox"/>
1.149	UBTU-22-654090	<input type="checkbox"/>	<input type="checkbox"/>
1.150	UBTU-22-654095	<input type="checkbox"/>	<input type="checkbox"/>
1.151	UBTU-22-654100	<input type="checkbox"/>	<input type="checkbox"/>
1.152	UBTU-22-654105	<input type="checkbox"/>	<input type="checkbox"/>
1.153	UBTU-22-654110	<input type="checkbox"/>	<input type="checkbox"/>
1.154	UBTU-22-654115	<input type="checkbox"/>	<input type="checkbox"/>
1.155	UBTU-22-654120	<input type="checkbox"/>	<input type="checkbox"/>
1.156	UBTU-22-654125	<input type="checkbox"/>	<input type="checkbox"/>
1.157	UBTU-22-654130	<input type="checkbox"/>	<input type="checkbox"/>
1.158	UBTU-22-654135	<input type="checkbox"/>	<input type="checkbox"/>
1.159	UBTU-22-654140	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.160	UBTU-22-654145	<input type="checkbox"/>	<input type="checkbox"/>
1.161	UBTU-22-654150	<input type="checkbox"/>	<input type="checkbox"/>
1.162	UBTU-22-654155	<input type="checkbox"/>	<input type="checkbox"/>
1.163	UBTU-22-654160	<input type="checkbox"/>	<input type="checkbox"/>
1.164	UBTU-22-654165	<input type="checkbox"/>	<input type="checkbox"/>
1.165	UBTU-22-654170	<input type="checkbox"/>	<input type="checkbox"/>
1.166	UBTU-22-654175	<input type="checkbox"/>	<input type="checkbox"/>
1.167	UBTU-22-654180	<input type="checkbox"/>	<input type="checkbox"/>
1.168	UBTU-22-654185	<input type="checkbox"/>	<input type="checkbox"/>
1.169	UBTU-22-654190	<input type="checkbox"/>	<input type="checkbox"/>
1.170	UBTU-22-654195	<input type="checkbox"/>	<input type="checkbox"/>
1.171	UBTU-22-654200	<input type="checkbox"/>	<input type="checkbox"/>
1.172	UBTU-22-654205	<input type="checkbox"/>	<input type="checkbox"/>
1.173	UBTU-22-654210	<input type="checkbox"/>	<input type="checkbox"/>
1.174	UBTU-22-654215	<input type="checkbox"/>	<input type="checkbox"/>
1.175	UBTU-22-654220	<input type="checkbox"/>	<input type="checkbox"/>
1.176	UBTU-22-654225	<input type="checkbox"/>	<input type="checkbox"/>
1.177	UBTU-22-654230	<input type="checkbox"/>	<input type="checkbox"/>
1.178	UBTU-22-654235	<input type="checkbox"/>	<input type="checkbox"/>
1.179	UBTU-22-671010	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.3	UBTU-22-212015	<input type="checkbox"/>	<input type="checkbox"/>
1.9	UBTU-22-214015	<input type="checkbox"/>	<input type="checkbox"/>
1.10	UBTU-22-215010	<input type="checkbox"/>	<input type="checkbox"/>
1.59	UBTU-22-255030	<input type="checkbox"/>	<input type="checkbox"/>
1.60	UBTU-22-255035	<input type="checkbox"/>	<input type="checkbox"/>
1.69	UBTU-22-271020	<input type="checkbox"/>	<input type="checkbox"/>
1.75	UBTU-22-411015	<input type="checkbox"/>	<input type="checkbox"/>
1.115	UBTU-22-651030	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	UBTU-22-211015	<input type="checkbox"/>	<input type="checkbox"/>
1.2	UBTU-22-212010	<input type="checkbox"/>	<input type="checkbox"/>
1.3	UBTU-22-212015	<input type="checkbox"/>	<input type="checkbox"/>
1.8	UBTU-22-214010	<input type="checkbox"/>	<input type="checkbox"/>
1.17	UBTU-22-232010	<input type="checkbox"/>	<input type="checkbox"/>
1.18	UBTU-22-232015	<input type="checkbox"/>	<input type="checkbox"/>
1.19	UBTU-22-232020	<input type="checkbox"/>	<input type="checkbox"/>
1.20	UBTU-22-232025	<input type="checkbox"/>	<input type="checkbox"/>
1.21	UBTU-22-232026	<input type="checkbox"/>	<input type="checkbox"/>
1.22	UBTU-22-232027	<input type="checkbox"/>	<input type="checkbox"/>
1.23	UBTU-22-232030	<input type="checkbox"/>	<input type="checkbox"/>
1.24	UBTU-22-232035	<input type="checkbox"/>	<input type="checkbox"/>
1.25	UBTU-22-232040	<input type="checkbox"/>	<input type="checkbox"/>
1.26	UBTU-22-232045	<input type="checkbox"/>	<input type="checkbox"/>
1.27	UBTU-22-232050	<input type="checkbox"/>	<input type="checkbox"/>
1.28	UBTU-22-232055	<input type="checkbox"/>	<input type="checkbox"/>
1.29	UBTU-22-232060	<input type="checkbox"/>	<input type="checkbox"/>
1.30	UBTU-22-232065	<input type="checkbox"/>	<input type="checkbox"/>
1.31	UBTU-22-232070	<input type="checkbox"/>	<input type="checkbox"/>
1.32	UBTU-22-232075	<input type="checkbox"/>	<input type="checkbox"/>
1.33	UBTU-22-232080	<input type="checkbox"/>	<input type="checkbox"/>
1.34	UBTU-22-232085	<input type="checkbox"/>	<input type="checkbox"/>
1.35	UBTU-22-232090	<input type="checkbox"/>	<input type="checkbox"/>
1.36	UBTU-22-232095	<input type="checkbox"/>	<input type="checkbox"/>
1.37	UBTU-22-232100	<input type="checkbox"/>	<input type="checkbox"/>
1.38	UBTU-22-232105	<input type="checkbox"/>	<input type="checkbox"/>
1.39	UBTU-22-232110	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.40	UBTU-22-232120	<input type="checkbox"/>	<input type="checkbox"/>
1.41	UBTU-22-232125	<input type="checkbox"/>	<input type="checkbox"/>
1.42	UBTU-22-232130	<input type="checkbox"/>	<input type="checkbox"/>
1.43	UBTU-22-232135	<input type="checkbox"/>	<input type="checkbox"/>
1.44	UBTU-22-232140	<input type="checkbox"/>	<input type="checkbox"/>
1.45	UBTU-22-232145	<input type="checkbox"/>	<input type="checkbox"/>
1.46	UBTU-22-251010	<input type="checkbox"/>	<input type="checkbox"/>
1.47	UBTU-22-251015	<input type="checkbox"/>	<input type="checkbox"/>
1.48	UBTU-22-251020	<input type="checkbox"/>	<input type="checkbox"/>
1.49	UBTU-22-251025	<input type="checkbox"/>	<input type="checkbox"/>
1.50	UBTU-22-251030	<input type="checkbox"/>	<input type="checkbox"/>
1.57	UBTU-22-255020	<input type="checkbox"/>	<input type="checkbox"/>
1.58	UBTU-22-255025	<input type="checkbox"/>	<input type="checkbox"/>
1.66	UBTU-22-255065	<input type="checkbox"/>	<input type="checkbox"/>
1.67	UBTU-22-271010	<input type="checkbox"/>	<input type="checkbox"/>
1.68	UBTU-22-271015	<input type="checkbox"/>	<input type="checkbox"/>
1.69	UBTU-22-271020	<input type="checkbox"/>	<input type="checkbox"/>
1.70	UBTU-22-271025	<input type="checkbox"/>	<input type="checkbox"/>
1.71	UBTU-22-271030	<input type="checkbox"/>	<input type="checkbox"/>
1.72	UBTU-22-291010	<input type="checkbox"/>	<input type="checkbox"/>
1.74	UBTU-22-411010	<input type="checkbox"/>	<input type="checkbox"/>
1.76	UBTU-22-411025	<input type="checkbox"/>	<input type="checkbox"/>
1.77	UBTU-22-411030	<input type="checkbox"/>	<input type="checkbox"/>
1.78	UBTU-22-411035	<input type="checkbox"/>	<input type="checkbox"/>
1.79	UBTU-22-411040	<input type="checkbox"/>	<input type="checkbox"/>
1.80	UBTU-22-411045	<input type="checkbox"/>	<input type="checkbox"/>
1.81	UBTU-22-412010	<input type="checkbox"/>	<input type="checkbox"/>
1.82	UBTU-22-412020	<input type="checkbox"/>	<input type="checkbox"/>
1.83	UBTU-22-412025	<input type="checkbox"/>	<input type="checkbox"/>
1.84	UBTU-22-412030	<input type="checkbox"/>	<input type="checkbox"/>
1.85	UBTU-22-412035	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.86	UBTU-22-431010	<input type="checkbox"/>	<input type="checkbox"/>
1.88	UBTU-22-432010	<input type="checkbox"/>	<input type="checkbox"/>
1.89	UBTU-22-432015	<input type="checkbox"/>	<input type="checkbox"/>
1.90	UBTU-22-611010	<input type="checkbox"/>	<input type="checkbox"/>
1.91	UBTU-22-611015	<input type="checkbox"/>	<input type="checkbox"/>
1.92	UBTU-22-611020	<input type="checkbox"/>	<input type="checkbox"/>
1.93	UBTU-22-611025	<input type="checkbox"/>	<input type="checkbox"/>
1.94	UBTU-22-611030	<input type="checkbox"/>	<input type="checkbox"/>
1.95	UBTU-22-611035	<input type="checkbox"/>	<input type="checkbox"/>
1.96	UBTU-22-611040	<input type="checkbox"/>	<input type="checkbox"/>
1.97	UBTU-22-611045	<input type="checkbox"/>	<input type="checkbox"/>
1.98	UBTU-22-611055	<input type="checkbox"/>	<input type="checkbox"/>
1.99	UBTU-22-611060	<input type="checkbox"/>	<input type="checkbox"/>
1.100	UBTU-22-611065	<input type="checkbox"/>	<input type="checkbox"/>
1.102	UBTU-22-612010	<input type="checkbox"/>	<input type="checkbox"/>
1.103	UBTU-22-612015	<input type="checkbox"/>	<input type="checkbox"/>
1.104	UBTU-22-612020	<input type="checkbox"/>	<input type="checkbox"/>
1.105	UBTU-22-612025	<input type="checkbox"/>	<input type="checkbox"/>
1.106	UBTU-22-612030	<input type="checkbox"/>	<input type="checkbox"/>
1.107	UBTU-22-612035	<input type="checkbox"/>	<input type="checkbox"/>
1.108	UBTU-22-612040	<input type="checkbox"/>	<input type="checkbox"/>
1.109	UBTU-22-631010	<input type="checkbox"/>	<input type="checkbox"/>
1.110	UBTU-22-631015	<input type="checkbox"/>	<input type="checkbox"/>
1.114	UBTU-22-651025	<input type="checkbox"/>	<input type="checkbox"/>
1.116	UBTU-22-651035	<input type="checkbox"/>	<input type="checkbox"/>
1.117	UBTU-22-652010	<input type="checkbox"/>	<input type="checkbox"/>
1.118	UBTU-22-652015	<input type="checkbox"/>	<input type="checkbox"/>
1.120	UBTU-22-653015	<input type="checkbox"/>	<input type="checkbox"/>
1.121	UBTU-22-653020	<input type="checkbox"/>	<input type="checkbox"/>
1.122	UBTU-22-653025	<input type="checkbox"/>	<input type="checkbox"/>
1.123	UBTU-22-653030	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.124	UBTU-22-653035	<input type="checkbox"/>	<input type="checkbox"/>
1.125	UBTU-22-653040	<input type="checkbox"/>	<input type="checkbox"/>
1.126	UBTU-22-653045	<input type="checkbox"/>	<input type="checkbox"/>
1.127	UBTU-22-653050	<input type="checkbox"/>	<input type="checkbox"/>
1.128	UBTU-22-653055	<input type="checkbox"/>	<input type="checkbox"/>
1.129	UBTU-22-653060	<input type="checkbox"/>	<input type="checkbox"/>
1.130	UBTU-22-653065	<input type="checkbox"/>	<input type="checkbox"/>
1.131	UBTU-22-653070	<input type="checkbox"/>	<input type="checkbox"/>
1.132	UBTU-22-653075	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	UBTU-22-211015	<input type="checkbox"/>	<input type="checkbox"/>
1.2	UBTU-22-212010	<input type="checkbox"/>	<input type="checkbox"/>
1.3	UBTU-22-212015	<input type="checkbox"/>	<input type="checkbox"/>
1.4	UBTU-22-213010	<input type="checkbox"/>	<input type="checkbox"/>
1.5	UBTU-22-213015	<input type="checkbox"/>	<input type="checkbox"/>
1.6	UBTU-22-213020	<input type="checkbox"/>	<input type="checkbox"/>
1.7	UBTU-22-213025	<input type="checkbox"/>	<input type="checkbox"/>
1.8	UBTU-22-214010	<input type="checkbox"/>	<input type="checkbox"/>
1.11	UBTU-22-215015	<input type="checkbox"/>	<input type="checkbox"/>
1.12	UBTU-22-215020	<input type="checkbox"/>	<input type="checkbox"/>
1.13	UBTU-22-215025	<input type="checkbox"/>	<input type="checkbox"/>
1.14	UBTU-22-215030	<input type="checkbox"/>	<input type="checkbox"/>
1.15	UBTU-22-215035	<input type="checkbox"/>	<input type="checkbox"/>
1.16	UBTU-22-231010	<input type="checkbox"/>	<input type="checkbox"/>
1.17	UBTU-22-232010	<input type="checkbox"/>	<input type="checkbox"/>
1.18	UBTU-22-232015	<input type="checkbox"/>	<input type="checkbox"/>
1.19	UBTU-22-232020	<input type="checkbox"/>	<input type="checkbox"/>
1.20	UBTU-22-232025	<input type="checkbox"/>	<input type="checkbox"/>
1.21	UBTU-22-232026	<input type="checkbox"/>	<input type="checkbox"/>
1.22	UBTU-22-232027	<input type="checkbox"/>	<input type="checkbox"/>
1.23	UBTU-22-232030	<input type="checkbox"/>	<input type="checkbox"/>
1.24	UBTU-22-232035	<input type="checkbox"/>	<input type="checkbox"/>
1.25	UBTU-22-232040	<input type="checkbox"/>	<input type="checkbox"/>
1.26	UBTU-22-232045	<input type="checkbox"/>	<input type="checkbox"/>
1.27	UBTU-22-232050	<input type="checkbox"/>	<input type="checkbox"/>
1.28	UBTU-22-232055	<input type="checkbox"/>	<input type="checkbox"/>
1.29	UBTU-22-232060	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.30	UBTU-22-232065	<input type="checkbox"/>	<input type="checkbox"/>
1.31	UBTU-22-232070	<input type="checkbox"/>	<input type="checkbox"/>
1.32	UBTU-22-232075	<input type="checkbox"/>	<input type="checkbox"/>
1.33	UBTU-22-232080	<input type="checkbox"/>	<input type="checkbox"/>
1.34	UBTU-22-232085	<input type="checkbox"/>	<input type="checkbox"/>
1.35	UBTU-22-232090	<input type="checkbox"/>	<input type="checkbox"/>
1.36	UBTU-22-232095	<input type="checkbox"/>	<input type="checkbox"/>
1.37	UBTU-22-232100	<input type="checkbox"/>	<input type="checkbox"/>
1.38	UBTU-22-232105	<input type="checkbox"/>	<input type="checkbox"/>
1.39	UBTU-22-232110	<input type="checkbox"/>	<input type="checkbox"/>
1.40	UBTU-22-232120	<input type="checkbox"/>	<input type="checkbox"/>
1.41	UBTU-22-232125	<input type="checkbox"/>	<input type="checkbox"/>
1.42	UBTU-22-232130	<input type="checkbox"/>	<input type="checkbox"/>
1.43	UBTU-22-232135	<input type="checkbox"/>	<input type="checkbox"/>
1.44	UBTU-22-232140	<input type="checkbox"/>	<input type="checkbox"/>
1.45	UBTU-22-232145	<input type="checkbox"/>	<input type="checkbox"/>
1.46	UBTU-22-251010	<input type="checkbox"/>	<input type="checkbox"/>
1.47	UBTU-22-251015	<input type="checkbox"/>	<input type="checkbox"/>
1.48	UBTU-22-251020	<input type="checkbox"/>	<input type="checkbox"/>
1.49	UBTU-22-251025	<input type="checkbox"/>	<input type="checkbox"/>
1.50	UBTU-22-251030	<input type="checkbox"/>	<input type="checkbox"/>
1.51	UBTU-22-252010	<input type="checkbox"/>	<input type="checkbox"/>
1.52	UBTU-22-252015	<input type="checkbox"/>	<input type="checkbox"/>
1.53	UBTU-22-252020	<input type="checkbox"/>	<input type="checkbox"/>
1.54	UBTU-22-253010	<input type="checkbox"/>	<input type="checkbox"/>
1.55	UBTU-22-255010	<input type="checkbox"/>	<input type="checkbox"/>
1.56	UBTU-22-255015	<input type="checkbox"/>	<input type="checkbox"/>
1.57	UBTU-22-255020	<input type="checkbox"/>	<input type="checkbox"/>
1.58	UBTU-22-255025	<input type="checkbox"/>	<input type="checkbox"/>
1.61	UBTU-22-255040	<input type="checkbox"/>	<input type="checkbox"/>
1.62	UBTU-22-255045	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.63	UBTU-22-255050	<input type="checkbox"/>	<input type="checkbox"/>
1.64	UBTU-22-255055	<input type="checkbox"/>	<input type="checkbox"/>
1.65	UBTU-22-255060	<input type="checkbox"/>	<input type="checkbox"/>
1.66	UBTU-22-255065	<input type="checkbox"/>	<input type="checkbox"/>
1.67	UBTU-22-271010	<input type="checkbox"/>	<input type="checkbox"/>
1.68	UBTU-22-271015	<input type="checkbox"/>	<input type="checkbox"/>
1.69	UBTU-22-271020	<input type="checkbox"/>	<input type="checkbox"/>
1.70	UBTU-22-271025	<input type="checkbox"/>	<input type="checkbox"/>
1.71	UBTU-22-271030	<input type="checkbox"/>	<input type="checkbox"/>
1.72	UBTU-22-291010	<input type="checkbox"/>	<input type="checkbox"/>
1.73	UBTU-22-291015	<input type="checkbox"/>	<input type="checkbox"/>
1.74	UBTU-22-411010	<input type="checkbox"/>	<input type="checkbox"/>
1.76	UBTU-22-411025	<input type="checkbox"/>	<input type="checkbox"/>
1.77	UBTU-22-411030	<input type="checkbox"/>	<input type="checkbox"/>
1.78	UBTU-22-411035	<input type="checkbox"/>	<input type="checkbox"/>
1.79	UBTU-22-411040	<input type="checkbox"/>	<input type="checkbox"/>
1.80	UBTU-22-411045	<input type="checkbox"/>	<input type="checkbox"/>
1.81	UBTU-22-412010	<input type="checkbox"/>	<input type="checkbox"/>
1.82	UBTU-22-412020	<input type="checkbox"/>	<input type="checkbox"/>
1.83	UBTU-22-412025	<input type="checkbox"/>	<input type="checkbox"/>
1.84	UBTU-22-412030	<input type="checkbox"/>	<input type="checkbox"/>
1.85	UBTU-22-412035	<input type="checkbox"/>	<input type="checkbox"/>
1.86	UBTU-22-431010	<input type="checkbox"/>	<input type="checkbox"/>
1.88	UBTU-22-432010	<input type="checkbox"/>	<input type="checkbox"/>
1.89	UBTU-22-432015	<input type="checkbox"/>	<input type="checkbox"/>
1.90	UBTU-22-611010	<input type="checkbox"/>	<input type="checkbox"/>
1.91	UBTU-22-611015	<input type="checkbox"/>	<input type="checkbox"/>
1.92	UBTU-22-611020	<input type="checkbox"/>	<input type="checkbox"/>
1.93	UBTU-22-611025	<input type="checkbox"/>	<input type="checkbox"/>
1.94	UBTU-22-611030	<input type="checkbox"/>	<input type="checkbox"/>
1.95	UBTU-22-611035	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.96	UBTU-22-611040	<input type="checkbox"/>	<input type="checkbox"/>
1.97	UBTU-22-611045	<input type="checkbox"/>	<input type="checkbox"/>
1.98	UBTU-22-611055	<input type="checkbox"/>	<input type="checkbox"/>
1.99	UBTU-22-611060	<input type="checkbox"/>	<input type="checkbox"/>
1.100	UBTU-22-611065	<input type="checkbox"/>	<input type="checkbox"/>
1.101	UBTU-22-611070	<input type="checkbox"/>	<input type="checkbox"/>
1.102	UBTU-22-612010	<input type="checkbox"/>	<input type="checkbox"/>
1.103	UBTU-22-612015	<input type="checkbox"/>	<input type="checkbox"/>
1.104	UBTU-22-612020	<input type="checkbox"/>	<input type="checkbox"/>
1.105	UBTU-22-612025	<input type="checkbox"/>	<input type="checkbox"/>
1.106	UBTU-22-612030	<input type="checkbox"/>	<input type="checkbox"/>
1.107	UBTU-22-612035	<input type="checkbox"/>	<input type="checkbox"/>
1.108	UBTU-22-612040	<input type="checkbox"/>	<input type="checkbox"/>
1.109	UBTU-22-631010	<input type="checkbox"/>	<input type="checkbox"/>
1.110	UBTU-22-631015	<input type="checkbox"/>	<input type="checkbox"/>
1.114	UBTU-22-651025	<input type="checkbox"/>	<input type="checkbox"/>
1.116	UBTU-22-651035	<input type="checkbox"/>	<input type="checkbox"/>
1.117	UBTU-22-652010	<input type="checkbox"/>	<input type="checkbox"/>
1.118	UBTU-22-652015	<input type="checkbox"/>	<input type="checkbox"/>
1.119	UBTU-22-653010	<input type="checkbox"/>	<input type="checkbox"/>
1.120	UBTU-22-653015	<input type="checkbox"/>	<input type="checkbox"/>
1.121	UBTU-22-653020	<input type="checkbox"/>	<input type="checkbox"/>
1.122	UBTU-22-653025	<input type="checkbox"/>	<input type="checkbox"/>
1.123	UBTU-22-653030	<input type="checkbox"/>	<input type="checkbox"/>
1.124	UBTU-22-653035	<input type="checkbox"/>	<input type="checkbox"/>
1.125	UBTU-22-653040	<input type="checkbox"/>	<input type="checkbox"/>
1.126	UBTU-22-653045	<input type="checkbox"/>	<input type="checkbox"/>
1.127	UBTU-22-653050	<input type="checkbox"/>	<input type="checkbox"/>
1.128	UBTU-22-653055	<input type="checkbox"/>	<input type="checkbox"/>
1.129	UBTU-22-653060	<input type="checkbox"/>	<input type="checkbox"/>
1.130	UBTU-22-653065	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.131	UBTU-22-653070	<input type="checkbox"/>	<input type="checkbox"/>
1.132	UBTU-22-653075	<input type="checkbox"/>	<input type="checkbox"/>
1.133	UBTU-22-654010	<input type="checkbox"/>	<input type="checkbox"/>
1.134	UBTU-22-654015	<input type="checkbox"/>	<input type="checkbox"/>
1.135	UBTU-22-654020	<input type="checkbox"/>	<input type="checkbox"/>
1.136	UBTU-22-654025	<input type="checkbox"/>	<input type="checkbox"/>
1.137	UBTU-22-654030	<input type="checkbox"/>	<input type="checkbox"/>
1.138	UBTU-22-654035	<input type="checkbox"/>	<input type="checkbox"/>
1.139	UBTU-22-654040	<input type="checkbox"/>	<input type="checkbox"/>
1.140	UBTU-22-654045	<input type="checkbox"/>	<input type="checkbox"/>
1.141	UBTU-22-654050	<input type="checkbox"/>	<input type="checkbox"/>
1.142	UBTU-22-654055	<input type="checkbox"/>	<input type="checkbox"/>
1.143	UBTU-22-654060	<input type="checkbox"/>	<input type="checkbox"/>
1.144	UBTU-22-654065	<input type="checkbox"/>	<input type="checkbox"/>
1.145	UBTU-22-654070	<input type="checkbox"/>	<input type="checkbox"/>
1.146	UBTU-22-654075	<input type="checkbox"/>	<input type="checkbox"/>
1.147	UBTU-22-654080	<input type="checkbox"/>	<input type="checkbox"/>
1.148	UBTU-22-654085	<input type="checkbox"/>	<input type="checkbox"/>
1.149	UBTU-22-654090	<input type="checkbox"/>	<input type="checkbox"/>
1.150	UBTU-22-654095	<input type="checkbox"/>	<input type="checkbox"/>
1.151	UBTU-22-654100	<input type="checkbox"/>	<input type="checkbox"/>
1.152	UBTU-22-654105	<input type="checkbox"/>	<input type="checkbox"/>
1.153	UBTU-22-654110	<input type="checkbox"/>	<input type="checkbox"/>
1.154	UBTU-22-654115	<input type="checkbox"/>	<input type="checkbox"/>
1.155	UBTU-22-654120	<input type="checkbox"/>	<input type="checkbox"/>
1.156	UBTU-22-654125	<input type="checkbox"/>	<input type="checkbox"/>
1.157	UBTU-22-654130	<input type="checkbox"/>	<input type="checkbox"/>
1.158	UBTU-22-654135	<input type="checkbox"/>	<input type="checkbox"/>
1.159	UBTU-22-654140	<input type="checkbox"/>	<input type="checkbox"/>
1.160	UBTU-22-654145	<input type="checkbox"/>	<input type="checkbox"/>
1.161	UBTU-22-654150	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.162	UBTU-22-654155	<input type="checkbox"/>	<input type="checkbox"/>
1.163	UBTU-22-654160	<input type="checkbox"/>	<input type="checkbox"/>
1.164	UBTU-22-654165	<input type="checkbox"/>	<input type="checkbox"/>
1.165	UBTU-22-654170	<input type="checkbox"/>	<input type="checkbox"/>
1.166	UBTU-22-654175	<input type="checkbox"/>	<input type="checkbox"/>
1.167	UBTU-22-654180	<input type="checkbox"/>	<input type="checkbox"/>
1.168	UBTU-22-654185	<input type="checkbox"/>	<input type="checkbox"/>
1.169	UBTU-22-654190	<input type="checkbox"/>	<input type="checkbox"/>
1.170	UBTU-22-654195	<input type="checkbox"/>	<input type="checkbox"/>
1.171	UBTU-22-654200	<input type="checkbox"/>	<input type="checkbox"/>
1.172	UBTU-22-654205	<input type="checkbox"/>	<input type="checkbox"/>
1.173	UBTU-22-654210	<input type="checkbox"/>	<input type="checkbox"/>
1.174	UBTU-22-654215	<input type="checkbox"/>	<input type="checkbox"/>
1.175	UBTU-22-654220	<input type="checkbox"/>	<input type="checkbox"/>
1.176	UBTU-22-654225	<input type="checkbox"/>	<input type="checkbox"/>
1.177	UBTU-22-654230	<input type="checkbox"/>	<input type="checkbox"/>
1.178	UBTU-22-654235	<input type="checkbox"/>	<input type="checkbox"/>
1.179	UBTU-22-671010	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	UBTU-22-211015	<input type="checkbox"/>	<input type="checkbox"/>
1.2	UBTU-22-212010	<input type="checkbox"/>	<input type="checkbox"/>
1.3	UBTU-22-212015	<input type="checkbox"/>	<input type="checkbox"/>
1.4	UBTU-22-213010	<input type="checkbox"/>	<input type="checkbox"/>
1.5	UBTU-22-213015	<input type="checkbox"/>	<input type="checkbox"/>
1.6	UBTU-22-213020	<input type="checkbox"/>	<input type="checkbox"/>
1.7	UBTU-22-213025	<input type="checkbox"/>	<input type="checkbox"/>
1.8	UBTU-22-214010	<input type="checkbox"/>	<input type="checkbox"/>
1.11	UBTU-22-215015	<input type="checkbox"/>	<input type="checkbox"/>
1.12	UBTU-22-215020	<input type="checkbox"/>	<input type="checkbox"/>
1.13	UBTU-22-215025	<input type="checkbox"/>	<input type="checkbox"/>
1.14	UBTU-22-215030	<input type="checkbox"/>	<input type="checkbox"/>
1.15	UBTU-22-215035	<input type="checkbox"/>	<input type="checkbox"/>
1.16	UBTU-22-231010	<input type="checkbox"/>	<input type="checkbox"/>
1.17	UBTU-22-232010	<input type="checkbox"/>	<input type="checkbox"/>
1.18	UBTU-22-232015	<input type="checkbox"/>	<input type="checkbox"/>
1.19	UBTU-22-232020	<input type="checkbox"/>	<input type="checkbox"/>
1.20	UBTU-22-232025	<input type="checkbox"/>	<input type="checkbox"/>
1.21	UBTU-22-232026	<input type="checkbox"/>	<input type="checkbox"/>
1.22	UBTU-22-232027	<input type="checkbox"/>	<input type="checkbox"/>
1.23	UBTU-22-232030	<input type="checkbox"/>	<input type="checkbox"/>
1.24	UBTU-22-232035	<input type="checkbox"/>	<input type="checkbox"/>
1.25	UBTU-22-232040	<input type="checkbox"/>	<input type="checkbox"/>
1.26	UBTU-22-232045	<input type="checkbox"/>	<input type="checkbox"/>
1.27	UBTU-22-232050	<input type="checkbox"/>	<input type="checkbox"/>
1.28	UBTU-22-232055	<input type="checkbox"/>	<input type="checkbox"/>
1.29	UBTU-22-232060	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.30	UBTU-22-232065	<input type="checkbox"/>	<input type="checkbox"/>
1.31	UBTU-22-232070	<input type="checkbox"/>	<input type="checkbox"/>
1.32	UBTU-22-232075	<input type="checkbox"/>	<input type="checkbox"/>
1.33	UBTU-22-232080	<input type="checkbox"/>	<input type="checkbox"/>
1.34	UBTU-22-232085	<input type="checkbox"/>	<input type="checkbox"/>
1.35	UBTU-22-232090	<input type="checkbox"/>	<input type="checkbox"/>
1.36	UBTU-22-232095	<input type="checkbox"/>	<input type="checkbox"/>
1.37	UBTU-22-232100	<input type="checkbox"/>	<input type="checkbox"/>
1.38	UBTU-22-232105	<input type="checkbox"/>	<input type="checkbox"/>
1.39	UBTU-22-232110	<input type="checkbox"/>	<input type="checkbox"/>
1.40	UBTU-22-232120	<input type="checkbox"/>	<input type="checkbox"/>
1.41	UBTU-22-232125	<input type="checkbox"/>	<input type="checkbox"/>
1.42	UBTU-22-232130	<input type="checkbox"/>	<input type="checkbox"/>
1.43	UBTU-22-232135	<input type="checkbox"/>	<input type="checkbox"/>
1.44	UBTU-22-232140	<input type="checkbox"/>	<input type="checkbox"/>
1.45	UBTU-22-232145	<input type="checkbox"/>	<input type="checkbox"/>
1.46	UBTU-22-251010	<input type="checkbox"/>	<input type="checkbox"/>
1.47	UBTU-22-251015	<input type="checkbox"/>	<input type="checkbox"/>
1.48	UBTU-22-251020	<input type="checkbox"/>	<input type="checkbox"/>
1.49	UBTU-22-251025	<input type="checkbox"/>	<input type="checkbox"/>
1.50	UBTU-22-251030	<input type="checkbox"/>	<input type="checkbox"/>
1.51	UBTU-22-252010	<input type="checkbox"/>	<input type="checkbox"/>
1.52	UBTU-22-252015	<input type="checkbox"/>	<input type="checkbox"/>
1.53	UBTU-22-252020	<input type="checkbox"/>	<input type="checkbox"/>
1.54	UBTU-22-253010	<input type="checkbox"/>	<input type="checkbox"/>
1.55	UBTU-22-255010	<input type="checkbox"/>	<input type="checkbox"/>
1.56	UBTU-22-255015	<input type="checkbox"/>	<input type="checkbox"/>
1.57	UBTU-22-255020	<input type="checkbox"/>	<input type="checkbox"/>
1.58	UBTU-22-255025	<input type="checkbox"/>	<input type="checkbox"/>
1.61	UBTU-22-255040	<input type="checkbox"/>	<input type="checkbox"/>
1.62	UBTU-22-255045	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.63	UBTU-22-255050	<input type="checkbox"/>	<input type="checkbox"/>
1.64	UBTU-22-255055	<input type="checkbox"/>	<input type="checkbox"/>
1.65	UBTU-22-255060	<input type="checkbox"/>	<input type="checkbox"/>
1.66	UBTU-22-255065	<input type="checkbox"/>	<input type="checkbox"/>
1.67	UBTU-22-271010	<input type="checkbox"/>	<input type="checkbox"/>
1.68	UBTU-22-271015	<input type="checkbox"/>	<input type="checkbox"/>
1.69	UBTU-22-271020	<input type="checkbox"/>	<input type="checkbox"/>
1.70	UBTU-22-271025	<input type="checkbox"/>	<input type="checkbox"/>
1.71	UBTU-22-271030	<input type="checkbox"/>	<input type="checkbox"/>
1.72	UBTU-22-291010	<input type="checkbox"/>	<input type="checkbox"/>
1.73	UBTU-22-291015	<input type="checkbox"/>	<input type="checkbox"/>
1.74	UBTU-22-411010	<input type="checkbox"/>	<input type="checkbox"/>
1.76	UBTU-22-411025	<input type="checkbox"/>	<input type="checkbox"/>
1.77	UBTU-22-411030	<input type="checkbox"/>	<input type="checkbox"/>
1.78	UBTU-22-411035	<input type="checkbox"/>	<input type="checkbox"/>
1.79	UBTU-22-411040	<input type="checkbox"/>	<input type="checkbox"/>
1.80	UBTU-22-411045	<input type="checkbox"/>	<input type="checkbox"/>
1.81	UBTU-22-412010	<input type="checkbox"/>	<input type="checkbox"/>
1.82	UBTU-22-412020	<input type="checkbox"/>	<input type="checkbox"/>
1.83	UBTU-22-412025	<input type="checkbox"/>	<input type="checkbox"/>
1.84	UBTU-22-412030	<input type="checkbox"/>	<input type="checkbox"/>
1.85	UBTU-22-412035	<input type="checkbox"/>	<input type="checkbox"/>
1.86	UBTU-22-431010	<input type="checkbox"/>	<input type="checkbox"/>
1.87	UBTU-22-431015	<input type="checkbox"/>	<input type="checkbox"/>
1.88	UBTU-22-432010	<input type="checkbox"/>	<input type="checkbox"/>
1.89	UBTU-22-432015	<input type="checkbox"/>	<input type="checkbox"/>
1.90	UBTU-22-611010	<input type="checkbox"/>	<input type="checkbox"/>
1.91	UBTU-22-611015	<input type="checkbox"/>	<input type="checkbox"/>
1.92	UBTU-22-611020	<input type="checkbox"/>	<input type="checkbox"/>
1.93	UBTU-22-611025	<input type="checkbox"/>	<input type="checkbox"/>
1.94	UBTU-22-611030	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.95	UBTU-22-611035	<input type="checkbox"/>	<input type="checkbox"/>
1.96	UBTU-22-611040	<input type="checkbox"/>	<input type="checkbox"/>
1.97	UBTU-22-611045	<input type="checkbox"/>	<input type="checkbox"/>
1.98	UBTU-22-611055	<input type="checkbox"/>	<input type="checkbox"/>
1.99	UBTU-22-611060	<input type="checkbox"/>	<input type="checkbox"/>
1.100	UBTU-22-611065	<input type="checkbox"/>	<input type="checkbox"/>
1.101	UBTU-22-611070	<input type="checkbox"/>	<input type="checkbox"/>
1.102	UBTU-22-612010	<input type="checkbox"/>	<input type="checkbox"/>
1.103	UBTU-22-612015	<input type="checkbox"/>	<input type="checkbox"/>
1.104	UBTU-22-612020	<input type="checkbox"/>	<input type="checkbox"/>
1.105	UBTU-22-612025	<input type="checkbox"/>	<input type="checkbox"/>
1.106	UBTU-22-612030	<input type="checkbox"/>	<input type="checkbox"/>
1.107	UBTU-22-612035	<input type="checkbox"/>	<input type="checkbox"/>
1.108	UBTU-22-612040	<input type="checkbox"/>	<input type="checkbox"/>
1.109	UBTU-22-631010	<input type="checkbox"/>	<input type="checkbox"/>
1.110	UBTU-22-631015	<input type="checkbox"/>	<input type="checkbox"/>
1.111	UBTU-22-651010	<input type="checkbox"/>	<input type="checkbox"/>
1.112	UBTU-22-651015	<input type="checkbox"/>	<input type="checkbox"/>
1.113	UBTU-22-651020	<input type="checkbox"/>	<input type="checkbox"/>
1.114	UBTU-22-651025	<input type="checkbox"/>	<input type="checkbox"/>
1.116	UBTU-22-651035	<input type="checkbox"/>	<input type="checkbox"/>
1.117	UBTU-22-652010	<input type="checkbox"/>	<input type="checkbox"/>
1.118	UBTU-22-652015	<input type="checkbox"/>	<input type="checkbox"/>
1.119	UBTU-22-653010	<input type="checkbox"/>	<input type="checkbox"/>
1.120	UBTU-22-653015	<input type="checkbox"/>	<input type="checkbox"/>
1.121	UBTU-22-653020	<input type="checkbox"/>	<input type="checkbox"/>
1.122	UBTU-22-653025	<input type="checkbox"/>	<input type="checkbox"/>
1.123	UBTU-22-653030	<input type="checkbox"/>	<input type="checkbox"/>
1.124	UBTU-22-653035	<input type="checkbox"/>	<input type="checkbox"/>
1.125	UBTU-22-653040	<input type="checkbox"/>	<input type="checkbox"/>
1.126	UBTU-22-653045	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.127	UBTU-22-653050	<input type="checkbox"/>	<input type="checkbox"/>
1.128	UBTU-22-653055	<input type="checkbox"/>	<input type="checkbox"/>
1.129	UBTU-22-653060	<input type="checkbox"/>	<input type="checkbox"/>
1.130	UBTU-22-653065	<input type="checkbox"/>	<input type="checkbox"/>
1.131	UBTU-22-653070	<input type="checkbox"/>	<input type="checkbox"/>
1.132	UBTU-22-653075	<input type="checkbox"/>	<input type="checkbox"/>
1.133	UBTU-22-654010	<input type="checkbox"/>	<input type="checkbox"/>
1.134	UBTU-22-654015	<input type="checkbox"/>	<input type="checkbox"/>
1.135	UBTU-22-654020	<input type="checkbox"/>	<input type="checkbox"/>
1.136	UBTU-22-654025	<input type="checkbox"/>	<input type="checkbox"/>
1.137	UBTU-22-654030	<input type="checkbox"/>	<input type="checkbox"/>
1.138	UBTU-22-654035	<input type="checkbox"/>	<input type="checkbox"/>
1.139	UBTU-22-654040	<input type="checkbox"/>	<input type="checkbox"/>
1.140	UBTU-22-654045	<input type="checkbox"/>	<input type="checkbox"/>
1.141	UBTU-22-654050	<input type="checkbox"/>	<input type="checkbox"/>
1.142	UBTU-22-654055	<input type="checkbox"/>	<input type="checkbox"/>
1.143	UBTU-22-654060	<input type="checkbox"/>	<input type="checkbox"/>
1.144	UBTU-22-654065	<input type="checkbox"/>	<input type="checkbox"/>
1.145	UBTU-22-654070	<input type="checkbox"/>	<input type="checkbox"/>
1.146	UBTU-22-654075	<input type="checkbox"/>	<input type="checkbox"/>
1.147	UBTU-22-654080	<input type="checkbox"/>	<input type="checkbox"/>
1.148	UBTU-22-654085	<input type="checkbox"/>	<input type="checkbox"/>
1.149	UBTU-22-654090	<input type="checkbox"/>	<input type="checkbox"/>
1.150	UBTU-22-654095	<input type="checkbox"/>	<input type="checkbox"/>
1.151	UBTU-22-654100	<input type="checkbox"/>	<input type="checkbox"/>
1.152	UBTU-22-654105	<input type="checkbox"/>	<input type="checkbox"/>
1.153	UBTU-22-654110	<input type="checkbox"/>	<input type="checkbox"/>
1.154	UBTU-22-654115	<input type="checkbox"/>	<input type="checkbox"/>
1.155	UBTU-22-654120	<input type="checkbox"/>	<input type="checkbox"/>
1.156	UBTU-22-654125	<input type="checkbox"/>	<input type="checkbox"/>
1.157	UBTU-22-654130	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.158	UBTU-22-654135	<input type="checkbox"/>	<input type="checkbox"/>
1.159	UBTU-22-654140	<input type="checkbox"/>	<input type="checkbox"/>
1.160	UBTU-22-654145	<input type="checkbox"/>	<input type="checkbox"/>
1.161	UBTU-22-654150	<input type="checkbox"/>	<input type="checkbox"/>
1.162	UBTU-22-654155	<input type="checkbox"/>	<input type="checkbox"/>
1.163	UBTU-22-654160	<input type="checkbox"/>	<input type="checkbox"/>
1.164	UBTU-22-654165	<input type="checkbox"/>	<input type="checkbox"/>
1.165	UBTU-22-654170	<input type="checkbox"/>	<input type="checkbox"/>
1.166	UBTU-22-654175	<input type="checkbox"/>	<input type="checkbox"/>
1.167	UBTU-22-654180	<input type="checkbox"/>	<input type="checkbox"/>
1.168	UBTU-22-654185	<input type="checkbox"/>	<input type="checkbox"/>
1.169	UBTU-22-654190	<input type="checkbox"/>	<input type="checkbox"/>
1.170	UBTU-22-654195	<input type="checkbox"/>	<input type="checkbox"/>
1.171	UBTU-22-654200	<input type="checkbox"/>	<input type="checkbox"/>
1.172	UBTU-22-654205	<input type="checkbox"/>	<input type="checkbox"/>
1.173	UBTU-22-654210	<input type="checkbox"/>	<input type="checkbox"/>
1.174	UBTU-22-654215	<input type="checkbox"/>	<input type="checkbox"/>
1.175	UBTU-22-654220	<input type="checkbox"/>	<input type="checkbox"/>
1.176	UBTU-22-654225	<input type="checkbox"/>	<input type="checkbox"/>
1.177	UBTU-22-654230	<input type="checkbox"/>	<input type="checkbox"/>
1.178	UBTU-22-654235	<input type="checkbox"/>	<input type="checkbox"/>
1.179	UBTU-22-671010	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.9	UBTU-22-214015	<input type="checkbox"/>	<input type="checkbox"/>
1.10	UBTU-22-215010	<input type="checkbox"/>	<input type="checkbox"/>
1.59	UBTU-22-255030	<input type="checkbox"/>	<input type="checkbox"/>
1.60	UBTU-22-255035	<input type="checkbox"/>	<input type="checkbox"/>
1.75	UBTU-22-411015	<input type="checkbox"/>	<input type="checkbox"/>
1.115	UBTU-22-651030	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: Change History

Date	Version	Changes for this version