

2 Services

While applying system updates and patches helps correct known vulnerabilities, one of the best ways to protect the system against as yet unreported vulnerabilities is to disable all services that are not required for normal system operation. This prevents the exploitation of vulnerabilities discovered at a later date. If a service is not enabled, it cannot be exploited. The actions in this section of the document provide guidance on some services which can be safely disabled and under which circumstances, greatly reducing the number of possible threats to the resulting system. Additionally, some services which should remain enabled but with secure configuration are covered as well as insecure service clients.

2.1 Configure Server Services

This section describes services that are installed on systems that specifically need to run these services. If any of these services are not required, it is recommended that the package be removed.

- **IF** - the package is required for a dependency:

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy
- Stop and mask the service and/or socket to reduce the potential attack surface

The following commands can be used to stop and mask the service and socket:

```
# systemctl stop <service_name>.socket <service_name>.service  
# systemctl mask <service_name>.socket <service_name>.service
```

Note: This should not be considered a comprehensive list of services not required for normal system operation. You may wish to consider additions to those listed here for your environment

2.1.1 Ensure autofs services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

Description:

autofs allows automatic mounting of devices, typically including CD/DVDs and USB drives.

Rationale:

With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in the filesystem even if they lacked permissions to mount it themselves.

Impact:

The use of portable hard drives is very common for workstation users. If your organization allows the use of portable storage or media on workstations and physical access controls to workstations is considered adequate there is little value add in turning off automounting.

There may be packages that are dependent on the **autofs** package. If the **autofs** package is removed, these dependent packages will be removed as well. Before removing the **autofs** package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the **autofs.service** leaving the **autofs** package installed.

Audit:

As a preference **autofs** should not be installed unless other packages depend on it. Run the following command to verify **autofs** is not installed:

```
# dpkg-query -s autofs &>/dev/null && echo "autofs is installed"
```

Nothing should be returned.

- OR -

- IF - the package is required for dependencies:

Run the following command to verify **autofs.service** is not enabled:

```
# systemctl is-enabled autofs.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned.

Run the following command to verify the **autofs.service** is not active:

```
# systemctl is-active autofs.service 2>/dev/null | grep '^active'
```

Nothing should be returned.

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop **autofs.service** and remove the **autofs** package:

```
# systemctl stop autofs.service  
# apt purge autofs
```

- OR -

- IF - the **autofs** package is required as a dependency:

Run the following commands to stop and mask **autofs.service**:

```
# systemctl stop autofs.service  
# systemctl mask autofs.service
```







References:

1. NIST SP 800-53 Rev. 5: SI-3, MP-7

Additional Information:

This control should align with the tolerance of the use of portable drives and optical media in the organization. On a server, requiring an admin to manually mount media can be part of defense-in-depth to reduce the risk of unapproved software or information being introduced or proprietary software or information being exfiltrated. If admins commonly use flash drives and Server access has sufficient physical controls, requiring manual mounting may not increase security.

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	8.5 <u>Configure Devices Not To Auto-run Content</u> Configure devices to not auto-run content from removable media.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000, T1203, T1203.000, T1211, T1211.000, T1212, T1212.000		

2.1.2 Ensure avahi daemon services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

Description:

Avahi is a free zeroconf implementation, including a system for multicast DNS/DNS-SD service discovery. Avahi allows programs to publish and discover services and hosts running on a local network with no specific configuration. For example, a user can plug a computer into a network and Avahi automatically finds printers to print to, files to look at and people to talk to, as well as network services running on the machine.

Rationale:

Automatic discovery of network services is not normally required for system functionality. It is recommended to remove this package to reduce the potential attack surface.

Impact:

There may be packages that are dependent on the **avahi** package. If the **avahi** package is removed, these dependent packages will be removed as well. Before removing the **avahi** package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the **avahi-daemon.socket** and **avahi-daemon.service** leaving the **avahi** package installed.

Audit:

Run the following command to verify **avahi-daemon** is not installed:

```
# dpkg-query -s avahi-daemon &>/dev/null && echo "avahi-daemon is installed"
```

Nothing should be returned.

- OR -

- IF - the **avahi** package is required as a dependency:

Run the following command to verify **avahi-daemon.socket** and **avahi-daemon.service** are not enabled:

```
# systemctl is-enabled avahi-daemon.socket avahi-daemon.service 2>/dev/null |  
grep 'enabled'
```

Nothing should be returned.

Run the following command to verify **avahi-daemon.socket** and **avahi-daemon.service** are not active:

```
# systemctl is-active avahi-daemon.socket avahi-daemon.service 2>/dev/null |  
grep '^active'
```

Nothing should be returned.

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop **avahi-daemon.socket** and **avahi-daemon.service**, and remove the **avahi-daemon** package:

```
# systemctl stop avahi-daemon.socket avahi-daemon.service  
# apt purge avahi-daemon
```

- OR -

- IF - the **avahi-daemon** package is required as a dependency:





Run the following commands to stop and mask the **avahi-daemon.socket** and **avahi-daemon.service**:

```
# systemctl stop avahi-daemon.socket avahi-daemon.service  
# systemctl mask avahi-daemon.socket avahi-daemon.service
```

References:

1. NIST SP 800-53 Rev. 5: SI-4

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.1.3 Ensure dhcp server services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Dynamic Host Configuration Protocol (DHCP) is a service that allows machines to be dynamically assigned IP addresses. There are two versions of the DHCP protocol **DHCPv4** and **DHCPv6**. At startup the server may be started for one or the other via the **-4** or **-6** arguments.

Rationale:

Unless a system is specifically set up to act as a DHCP server, it is recommended that this package be removed to reduce the potential attack surface.

Impact:

There may be packages that are dependent on the **isc-dhcp-server** package. If the **isc-dhcp-server** package is removed, these dependent packages will be removed as well. Before removing the **isc-dhcp-server** package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the **isc-dhcp-server.service** and **isc-dhcp-server6.service** leaving the **isc-dhcp-server** package installed.

Audit:

Run the following commands to verify **isc-dhcp-server** is not installed:

```
# dpkg-query -s isc-dhcp-server &>/dev/null && echo "isc-dhcp-server is installed"
```

Nothing should be returned.

- OR -

- IF - the package is required for dependencies:

Run the following command to verify **isc-dhcp-server.service** and **isc-dhcp-server6.service** are not enabled:

```
# systemctl is-enabled isc-dhcp-server.service isc-dhcp-server6.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned.

Run the following command to verify **isc-dhcp-server.service** and **isc-dhcp-server6.service** are not active:

```
# systemctl is-active isc-dhcp-server.service isc-dhcp-server6.service 2>/dev/null | grep '^active'
```

Nothing should be returned.

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop **isc-dhcp-server.service** and **isc-dhcp-server6.service** and remove the **isc-dhcp-server** package:

```
# systemctl stop isc-dhcp-server.service isc-dhcp-server6.service  
# apt purge isc-dhcp-server
```

- OR -

- IF - the **isc-dhcp-server** package is required as a dependency:





Run the following commands to stop and mask **isc-dhcp-server.service** and **isc-dhcp-server6.service**:

```
# systemctl stop isc-dhcp-server.service isc-dhcp-server6.service  
# systemctl mask isc-dhcp-server isc-dhcp-server6.service
```

References:

1. More detailed documentation on DHCP is available at <http://www.isc.org/software/dhcp>.
2. NIST SP 800-53 Rev. 5: CM-7

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.1.4 Ensure dns server services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Domain Name System (DNS) is a hierarchical naming system that maps names to IP addresses for computers, services and other resources connected to a network.

Note: `bind9` is the package and `bind.service` is the alias for `named.service`.

Rationale:

Unless a system is specifically designated to act as a DNS server, it is recommended that the package be deleted to reduce the potential attack surface.

Impact:

There may be packages that are dependent on the `bind9` package. If the `bind9` package is removed, these dependent packages will be removed as well. Before removing the `bind9` package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask `named.service` leaving the `bind9` package installed.

Audit:

Run the following command to verify **bind9** is not installed:

```
# dpkg-query -s bind9 &>/dev/null && echo "bind9 is installed"
```

Nothing should be returned.

- OR -

- IF - the package is required for dependencies:

Run the following command to verify **named.service** is not enabled:

```
# systemctl is-enabled named.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned

Run the following command to verify the **named.service** is not active:

```
# systemctl is-active named.service 2>/dev/null | grep '^active'
```

Nothing should be returned

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop **named.service** and remove the **bind9** package:

```
# systemctl stop named.service  
# apt purge bind9
```

- OR -

- IF - the **bind9** package is required as a dependency:





Run the following commands to stop and mask **bind9.service**:

```
# systemctl stop named.service  
# systemctl mask named.service
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.1.5 Ensure dnsmasq services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

dnsmasq is a lightweight tool that provides DNS caching, DNS forwarding and DHCP (Dynamic Host Configuration Protocol) services.

Rationale:

Unless a system is specifically designated to act as a DNS caching, DNS forwarding and/or DHCP server, it is recommended that the package be removed to reduce the potential attack surface.

Impact:

There may be packages that are dependent on the **dnsmasq** package. If the **dnsmasq** package is removed, these dependent packages will be removed as well. Before removing the **dnsmasq** package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the **dnsmasq.service** leaving the **dnsmasq** package installed.

Audit:

Run one of the following commands to verify **dnsmasq** is not installed:

```
# dpkg-query -s dnsmasq &>/dev/null && echo "dnsmasq is installed"
```

Nothing should be returned.

- **OR** -

- **IF** - the package is required for dependencies:

Run the following command to verify **dnsmasq.service** is not enabled:

```
# systemctl is-enabled dnsmasq.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned.

Run the following command to verify the **dnsmasq.service** is not active:

```
# systemctl is-active dnsmasq.service 2>/dev/null | grep '^active'
```

Nothing should be returned.

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop **dnsmasq.service** and remove **dnsmasq** package:

```
# systemctl stop dnsmasq.service
# apt purge dnsmasq
```

- OR -

- IF - the **dnsmasq** package is required as a dependency:

Run the following commands to stop and mask the **dnsmasq.service**:

```
# systemctl stop dnsmasq.service
# systemctl mask dnsmasq.service
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.1.6 Ensure ftp server services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The File Transfer Protocol (FTP) provides networked computers with the ability to transfer files. **vsftpd** is the Very Secure File Transfer Protocol Daemon.

Rationale:

FTP does not protect the confidentiality of data or authentication credentials. It is recommended SFTP be used if file transfer is required. Unless there is a need to run the system as a FTP server (for example, to allow anonymous downloads), it is recommended that the package be deleted to reduce the potential attack surface.

Impact:

There may be packages that are dependent on the **vsftpd** package. If the **vsftpd** package is removed, these dependent packages will be removed as well. Before removing the **vsftpd** package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the **vsftpd.service** leaving the **vsftpd** package installed.

Audit:

Run the following command to verify **vsftpd** is not installed:

```
# dpkg-query -s vsftpd &>/dev/null && echo "vsftpd is installed"
```

Nothing should be returned.

- OR -

- IF - the package is required for dependencies:

Run the following command to verify **vsftpd** service is not enabled:

```
# systemctl is-enabled vsftpd.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned.

Run the following command to verify the **vsftpd** service is not active:

```
# systemctl is-active vsftpd.service 2>/dev/null | grep '^active'
```

Nothing should be returned.

Note:

- Other ftp server packages may exist. They should also be audited, if not required and authorized by local site policy
- If the package is required for a dependency:
 - Ensure the dependent package is approved by local site policy
 - Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop **vsftpd.service** and remove the **vsftpd** package:

```
# systemctl stop vsftpd.service  
# apt purge vsftpd
```

- OR -

- IF - the **vsftpd** package is required as a dependency:

Run the following commands to stop and mask the **vsftpd.service**:

```
# systemctl stop vsftpd.service  
# systemctl mask vsftpd.service
```

Note: Other ftp server packages may exist. If not required and authorized by local site policy, they should also be removed. If the package is required for a dependency, the service should be stopped and masked.





References:

1. NIST SP 800-53 Rev. 5: CM-7

Additional Information:

Additional FTP servers also exist and should be audited.

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.1.7 Ensure ldap server services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Lightweight Directory Access Protocol (LDAP) was introduced as a replacement for NIS/YP. It is a service that provides a method for looking up information from a central database.

Rationale:

If the system will not need to act as an LDAP server, it is recommended that the software be removed to reduce the potential attack surface.

Impact:

There may be packages that are dependent on the **slapd** package. If the **slapd** package is removed, these dependent packages will be removed as well. Before removing the **slapd** package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the **slapd.service** leaving the **slapd** package installed.

Audit:

Run the following command to verify **slapd** is not installed:

```
# dpkg-query -s slapd &>/dev/null && echo "slapd is installed"
```

Nothing should be returned.

- **OR** -

- **IF** - the package is required for dependencies:

Run the following command to verify **slapd.service** is not enabled:

```
# systemctl is-enabled slapd.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned.

Run the following command to verify **slapd.service** is not active:

```
# systemctl is-active slapd.service 2>/dev/null | grep '^active'
```

Nothing should be returned.

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop **slapd.service** and remove the **slapd** package:

```
# systemctl stop slapd.service
# apt purge slapd
```

- OR -

- IF - the **slapd** package is required as a dependency:





Run the following commands to stop and mask **slapd.service**:

```
# systemctl stop slapd.service
# systemctl mask slapd.service
```

References:

1. For more detailed documentation on OpenLDAP, go to the project homepage at <http://www.openldap.org>.
2. NIST SP 800-53 Rev. 5: CM-7

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.1.8 Ensure message access server services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`dovecot-imapd` and `dovecot-pop3d` are an open source IMAP and POP3 server for Linux based systems.

Rationale:

Unless POP3 and/or IMAP servers are to be provided by this system, it is recommended that the package be removed to reduce the potential attack surface.

Note: Several IMAP/POP3 servers exist and can use other service names. These should also be audited and the packages removed if not required.

Impact:

There may be packages that are dependent on `dovecot-imapd` and/or `dovecot-pop3d` packages. If `dovecot-imapd` and `dovecot-pop3d` packages are removed, these dependent packages will be removed as well. Before removing `dovecot-imapd` and/or `dovecot-pop3d` packages, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask `dovecot.socket` and `dovecot.service` leaving `dovecot-imapd` and/or `dovecot-pop3d` packages installed.

Audit:

Run the following command to verify **dovecot-imapd** and **dovecot-pop3d** are not installed:

```
# dpkg-query -s dovecot-imapd &>/dev/null && echo "dovecot-imapd is installed"
```

Nothing should be returned.

```
# dpkg-query -s dovecot-pop3d &>/dev/null && echo "dovecot-pop3d is installed"
```

Nothing should be returned.

- OR -

- IF - a package is installed **and** is required for dependencies:

Run the following commands to verify **dovecot.socket** and **dovecot.service** are not enabled:

```
# systemctl is-enabled dovecot.socket dovecot.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned.

Run the following command to verify **dovecot.socket** and **dovecot.service** are not active:

```
# systemctl is-active dovecot.socket dovecot.service 2>/dev/null | grep '^active'
```

Nothing should be returned.

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run one of the following commands to remove **dovecot-imapd** and **dovecot-pop3d**:
Run the following commands to stop **dovecot.socket** and **dovecot.service**, and remove the **dovecot-imapd** and **dovecot-pop3d** packages:

```
# systemctl stop dovecot.socket dovecot.service
# apt purge dovecot-imapd dovecot-pop3d
```

- OR -

- IF - a package is installed **and** is required for dependencies:

Run the following commands to stop and mask **dovecot.socket** and **dovecot.service**:

```
# systemctl stop dovecot.socket dovecot.service
# systemctl mask dovecot.socket dovecot.service
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

Additional Information:

Several IMAP/POP3 servers exist and can use other service names. **courier-imap** and **cyrus-imap** are example services that provide a mail server. These and other services should also be audited.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software 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 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.1.9 Ensure network file system services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Network File System (NFS) is one of the first and most widely distributed file systems in the UNIX environment. It provides the ability for systems to mount file systems of other servers through the network.

Rationale:

If the system does not export NFS shares, it is recommended that the `nfs-kernel-server` package be removed to reduce the remote attack surface.

Impact:

There may be packages that are dependent on the `nfs-kernel-server` package. If the `nfs-kernel-server` package is removed, these dependent packages will be removed as well. Before removing the `nfs-kernel-server` package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the `nfs-server.service` leaving the `nfs-kernel-server` package installed.

Audit:

Run the following command to verify **nfs-kernel-server** is not installed:

```
# dpkg-query -s nfs-kernel-server &>/dev/null && echo "nfs-kernel-server is installed"
```

Nothing should be returned.

- OR -

- IF - package is required for dependencies:

Run the following command to verify that the **nfs-server.service** is not enabled:

```
# systemctl is-enabled nfs-server.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned.

Run the following command to verify the **nfs-server.service** is not active:

```
# systemctl is-active nfs-server.service 2>/dev/null | grep '^active'
```

Nothing should be returned.

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following command to stop **nfs-server.service** and remove **nfs-kernel-server** package:

```
# systemctl stop nfs-server.service  
# apt purge nfs-kernel-server
```

- OR -

- IF - the **nfs-kernel-server** package is required as a dependency:





Run the following commands to stop and mask the **nfs-server.service**:

```
# systemctl stop nfs-server.service  
# systemctl mask nfs-server.service
```

References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-7

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1005, T1005.000, T1039, T1039.000, T1083, T1083.000, T1135, T1135.000, T1210, T1210.000	TA0008	M1042

2.1.10 Ensure nis server services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Network Information Service (NIS) (formally known as Yellow Pages) is a client-server directory service protocol for distributing system configuration files. The NIS server is a collection of programs that allow for the distribution of configuration files. The NIS client (**ypbind**) was used to bind a machine to an NIS server and receive the distributed configuration files.

Rationale:

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

Impact:

There may be packages that are dependent on the **ypserv** package. If the **ypserv** package is removed, these dependent packages will be removed as well. Before removing the **ypserv** package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the **ypserv.service** leaving the **ypserv** package installed.

Audit:

Run the following command to verify **ypserv** is not installed:

```
# dpkg-query -s ypserv &>/dev/null && echo "ypserv is installed"
```

Nothing should be returned.

- OR -

- IF - the package is required for dependencies:

Run the following command to verify **ypserv.service** is not enabled:

```
# systemctl is-enabled ypserv.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned.

Run the following command to verify **ypserv.service** is not active:

```
# systemctl is-active ypserv.service 2>/dev/null | grep '^active'
```

Nothing should be returned.

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop **ypserv.service** and remove **ypserv** package:

```
# systemctl stop ypserv.service  
# apt purge ypserv
```

- OR -

- IF - the **ypserv** package is required as a dependency:





Run the following commands to stop and mask **ypserv.service**:

```
# systemctl stop ypserv.service  
# systemctl mask ypserv.service
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.1.11 Ensure print server services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

Description:

The Common Unix Print System (CUPS) provides the ability to print to both local and network printers. A system running CUPS can also accept print jobs from remote systems and print them to local printers. It also provides a web based remote administration capability.

Rationale:

If the system does not need to print jobs or accept print jobs from other systems, it is recommended that CUPS be removed to reduce the potential attack surface.

Impact:

Removing the cups package, or disabling `cups.socket` and/or `cups.service` will prevent printing from the system, a common task for workstation systems.

There may be packages that are dependent on the `cups` package. If the `cups` package is removed, these dependent packages will be removed as well. Before removing the `cups` package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask `cups.socket` and `cups.service` leaving the `cups` package installed.

Audit:

Run the following command to verify **cups** is not Installed:

```
# dpkg-query -s cups &>/dev/null && echo "cups is installed"
```

Nothing should be returned.

- OR -

- IF - the **cups** package is required as a dependency:

Run the following command to verify the **cups.socket** and **cups.service** are not enabled:

```
# systemctl is-enabled cups.socket cups.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned.

Run the following command to verify the **cups.socket** and **cups.service** are not active:

```
# systemctl is-active cups.socket cups.service 2>/dev/null | grep '^active'
```

Nothing should be returned.

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop **cups.socket** and **cups.service**, and remove the **cups** package:

```
# systemctl stop cups.socket cups.service  
# apt purge cups
```

- OR -

- IF - the **cups** package is required as a dependency:





Run the following commands to stop and mask the **cups.socket** and **cups.service**:

```
# systemctl stop cups.socket cups.service  
# systemctl mask cups.socket cups.service
```

References:

1. <http://www.cups.org>
2. NIST SP 800-53 Rev. 5: CM-7

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.1.12 Ensure rpcbind services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `rpcbind` utility maps RPC services to the ports on which they listen. RPC processes notify `rpcbind` when they start, registering the ports they are listening on and the RPC program numbers they expect to serve. The client system then contacts `rpcbind` on the server with a particular RPC program number. The `rpcbind.service` redirects the client to the proper port number so it can communicate with the requested service.

Portmapper is an RPC service, which always listens on tcp and udp 111, and is used to map other RPC services (such as nfs, nlockmgr, quotad, mountd, etc.) to their corresponding port number on the server. When a remote host makes an RPC call to that server, it first consults with portmap to determine where the RPC server is listening.

Rationale:

A small request (~82 bytes via UDP) sent to the Portmapper generates a large response (7x to 28x amplification), which makes it a suitable tool for DDoS attacks. If `rpcbind` is not required, it is recommended to remove `rpcbind` package to reduce the potential attack surface.

Impact:

Many of the libvirt packages used by Enterprise Linux virtualization, and the `nfs-utils` package used for The Network File System (NFS), are dependent on the `rpcbind` package. If the `rpcbind` package is removed, these dependent packages will be removed as well. Before removing the `rpcbind` package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the `rpcbind.socket` and `rpcbind.service` leaving the `rpcbind` package installed.

Audit:

Run the following command to verify **rpcbind** package is not installed:

```
# dpkg-query -s rpcbind &>/dev/null && echo "rpcbind is installed"
```

Nothing should be returned.

- OR -

- IF - the **rpcbind** package is required as a dependency:

Run the following command to verify **rpcbind.socket** and **rpcbind.service** are not enabled:

```
# systemctl is-enabled rpcbind.socket rpcbind.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned.

Run the following command to verify **rpcbind.socket** and **rpcbind.service** are not active:

```
# systemctl is-active rpcbind.socket rpcbind.service 2>/dev/null | grep '^active'
```

Nothing should be returned.

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop **rpcbind.socket** and **rpcbind.service**, and remove the **rpcbind** package:

```
# systemctl stop rpcbind.socket rpcbind.service  
# apt purge rpcbind
```

- OR -

- IF - the **rpcbind** package is required as a dependency:





Run the following commands to stop and mask the **rpcbind.socket** and **rpcbind.service**:

```
# systemctl stop rpcbind.socket rpcbind.service  
# systemctl mask rpcbind.socket rpcbind.service
```

References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-7

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1498, T1498.002, T1543, T1543.002	TA0008	M1042

2.1.13 Ensure rsync services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The **rsync** service can be used to synchronize files between systems over network links.

Rationale:

rsync.service presents a security risk as the **rsync** protocol is unencrypted.

The **rsync** package should be removed to reduce the attack area of the system.

Impact:

There may be packages that are dependent on the **rsync** package. If the **rsync** package is removed, these dependent packages will be removed as well. Before removing the **rsync** package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask **rsync.service** leaving the **rsync** package installed.

Audit:

Run the following command to verify **rsync** is not installed:

```
# dpkg-query -s rsync &>/dev/null && echo "rsync is installed"
```

Nothing should be returned.

- **OR** -

- **IF** - the **rsync** package is required as a dependency:

Run the following command to verify **rsync.service** is not enabled:

```
# systemctl is-enabled rsync.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned.

Run the following command to verify **rsync.service** is not active:

```
# systemctl is-active rsync.service 2>/dev/null | grep '^active'
```

Nothing should be returned.

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop **rsync.service**, and remove the **rsync** package:

```
# systemctl stop rsync.service
# apt purge rsync
```

- OR -

- IF - the **rsync** package is required as a dependency:

Run the following commands to stop and mask **rsync.service**:

```
# systemctl stop rsync.service
# systemctl mask rsync.service
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1105, T1105.000, T1203, T1203.000, T1210, T1210.000, T1543, T1543.002, T1570, T1570.000	TA0008	M1042

2.1.14 Ensure samba file server services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Samba daemon allows system administrators to configure their Linux systems to share file systems and directories with Windows desktops. Samba will advertise the file systems and directories via the Server Message Block (SMB) protocol. Windows desktop users will be able to mount these directories and file systems as letter drives on their systems.

Rationale:

If there is no need to mount directories and file systems to Windows systems, then this service should be deleted to reduce the potential attack surface.

Impact:

There may be packages that are dependent on the **samba** package. If the **samba** package is removed, these dependent packages will be removed as well. Before removing the **samba** package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the **smbd.service** leaving the **samba** package installed.

Audit:

Run the following command to verify **samba** is not installed:

```
# dpkg-query -s samba &>/dev/null && echo "samba is installed"
```

Nothing should be returned.

- **OR** -

- **IF** - the package is required for dependencies:

Run the following command to verify **smbd.service** is not enabled:

```
# systemctl is-enabled smbd.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned.

Run the following command to verify the **smbd.service** is not active:

```
# systemctl is-active smbd.service 2>/dev/null | grep '^active'
```

Nothing should be returned.

Remediation:

Run the following commands to stop **smbd.service** and remove **samba** package:

```
# systemctl stop smbd.service
# apt purge samba
```

- OR -

- IF - the **samba** package is required as a dependency:

Run the following commands to stop and mask the **smbd.service**:

```
# systemctl stop smbd.service
# systemctl mask smbd.service
```

References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-7

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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1005, T1005.000, T1039, T1039.000, T1083, T1083.000, T1135, T1135.000, T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	

2.1.15 Ensure snmp services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Simple Network Management Protocol (SNMP) is a widely used protocol for monitoring the health and welfare of network equipment, computer equipment and devices like UPSs.

Net-SNMP is a suite of applications used to implement SNMPv1 (RFC 1157), SNMPv2 (RFCs 1901-1908), and SNMPv3 (RFCs 3411-3418) using both IPv4 and IPv6.

Support for SNMPv2 classic (a.k.a. "SNMPv2 historic" - RFCs 1441-1452) was dropped with the 4.0 release of the UCD-snmp package.

The Simple Network Management Protocol (SNMP) server is used to listen for SNMP commands from an SNMP management system, execute the commands or collect the information and then send results back to the requesting system.

Rationale:

The SNMP server can communicate using **SNMPv1**, which transmits data in the clear and does not require authentication to execute commands. **SNMPv3** replaces the simple/clear text password sharing used in **SNMPv2** with more securely encoded parameters. If the the SNMP service is not required, the **snmpd** package should be removed to reduce the attack surface of the system.

Note: If SNMP is required:

- The server should be configured for **SNMP v3** only. **User Authentication** and **Message Encryption** should be configured.
- If **SNMP v2** is **absolutely** necessary, modify the community strings' values.

Impact:

There may be packages that are dependent on the **snmpd** package. If the **snmpd** package is removed, these packages will be removed as well.

Before removing the **snmpd** package, review any dependent packages to determine if they are required on the system. If a dependent package is required, stop and mask the **snmpd.service** leaving the **snmpd** package installed.

Audit:

Run the following command to verify **snmpd** is not installed:

```
# dpkg-query -s snmpd &>/dev/null && echo "snmpd is installed"
```

Nothing should be returned.

- OR -

- IF - the package is required for dependencies:

Run the following command to verify the **snmpd.service** is not enabled:

```
# systemctl is-enabled snmpd.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned.

Run the following command to verify the **snmpd.service** is not active:

```
# systemctl is-active snmpd.service 2>/dev/null | grep '^active'
```

Nothing should be returned.

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop **snmpd.service** and remove the **snmpd** package:

```
# systemctl stop snmpd.service  
# apt purge snmpd
```

- OR - If the package is required for dependencies:





Run the following commands to stop and mask the **snmpd.service**:

```
# systemctl stop snmpd.service  
# systemctl mask snmpd.service
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.1.16 Ensure tftp server services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Trivial File Transfer Protocol (TFTP) is a simple protocol for exchanging files between two TCP/IP machines. TFTP servers allow connections from a TFTP Client for sending and receiving files.

Rationale:

Unless there is a need to run the system as a TFTP server, it is recommended that the package be removed to reduce the potential attack surface.

TFTP does not have built-in encryption, access control or authentication. This makes it very easy for an attacker to exploit TFTP to gain access to files

Impact:

TFTP is often used to provide files for network booting such as for PXE based installation of servers.

There may be packages that are dependent on the `tftpd-hpa` package. If the `tftpd-hpa` package is removed, these dependent packages will be removed as well. Before removing the `tftpd-hpa` package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask `tftpd-hpa.service` leaving the `tftpd-hpa` package installed.

Audit:

Run the following command to verify **tftpd-hpa** is not installed:

```
# dpkg-query -s tftpd-hpa &>/dev/null && echo "tftpd-hpa is installed"
```

Nothing should be returned.

- OR -

- IF - the package is required for dependencies:

Run the following command to verify **tftpd-hpa.service** is not enabled:

```
# systemctl is-enabled tftpd-hpa.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned.

Run the following command to verify the **tftpd-hpa.service** is not active:

```
# systemctl is-active tftpd-hpa.service 2>/dev/null | grep '^active'
```

Nothing should be returned.

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop **tftpd-hpa.service**, and remove the **tftpd-hpa** package:

```
# systemctl stop tftpd-hpa.service  
# apt purge tftpd-hpa
```

- OR -

- IF - the **tftpd-hpa** package is required as a dependency:





Run the following commands to stop and mask **tftpd-hpa.service**:

```
# systemctl stop tftpd-hpa.service  
# systemctl mask tftpd-hpa.service
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.1.17 Ensure web proxy server services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Squid is a standard proxy server used in many distributions and environments.

Rationale:

Unless a system is specifically set up to act as a proxy server, it is recommended that the squid package be removed to reduce the potential attack surface.

Note: Several HTTP proxy servers exist. These should be checked and removed unless required.

Impact:

There may be packages that are dependent on the **squid** package. If the **squid** package is removed, these dependent packages will be removed as well. Before removing the **squid** package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the **squid.service** leaving the **squid** package installed.

Audit:

Run the following command to verify **squid** is not installed:

```
# dpkg-query -s squid &>/dev/null && echo "squid is installed"
```

Nothing should be returned.

- OR -

- IF - the package is required for dependencies:

Run the following command to verify **squid.service** is not enabled:

```
# systemctl is-enabled squid.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned.

Run the following command to verify the **squid.service** is not active:

```
# systemctl is-active squid.service 2>/dev/null | grep '^active'
```

Nothing should be returned.

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop **squid.service** and remove the **squid** package:

```
# systemctl stop squid.service  
# apt purge squid
```

- OR - If the **squid** package is required as a dependency:

Run the following commands to stop and mask the **squid.service**:

```
# systemctl stop squid.service  
# systemctl mask squid.service
```





References:

1. NIST SP 800-53 Rev. 5: CM-7

Additional Information:

Several HTTP proxy servers exist. These and other services should be checked

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.1.18 Ensure web server services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Web servers provide the ability to host web site content.

Rationale:

Unless there is a local site approved requirement to run a web server service on the system, web server packages should be removed to reduce the potential attack surface.

Impact:

Removal of web server packages will remove that ability for the server to host web services.

- **IF** - the web server package is required for a dependency, any related service or socket should be stopped and masked.

Note: If the remediation steps to mask a service are followed and that package is not installed on the system, the service and/or socket will still be masked. If the package is installed due to an approved requirement to host a web server, the associated service and/or socket would need to be unmasked before it could be enabled and/or started.

Audit:

Run the following command to verify **apache2** is not installed:

```
# dpkg-query -s apache2 &>/dev/null && echo "apache2 is installed"
```

Nothing should be returned.

Run the following command to verify **nginx** is not installed:

```
# dpkg-query -s nginx &>/dev/null && echo "nginx is installed"
```

Nothing should be returned.

- OR -

- IF - a package is installed **and** is required for dependencies:

Run the following command to verify **apache2.socket**, **apache2.service**, and **nginx.service** are not enabled:

```
# systemctl is-enabled apache2.socket apache2.service nginx.service  
2>/dev/null | grep 'enabled'
```

Nothing should be returned.

Run the following command to verify **apache2.socket**, **apache2.service**, and **nginx.service** are not active:

```
# systemctl is-active apache2.socket apache2.service nginx.service  
2>/dev/null | grep '^active'
```

Nothing should be returned.

Note:

- Other web server packages may exist. They should also be audited, if not required and authorized by local site policy
- If the package is required for a dependency:
 - Ensure the dependent package is approved by local site policy
 - Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop **httpd.socket**, **httpd.service**, and **nginx.service**, and remove **apache2** and **nginx** packages:

```
# systemctl stop apache2.socket apache2.service nginx.service
# apt purge apache2 nginx
```

- OR -

- IF - a package is installed **and** is required for dependencies:

Run the following commands to stop and mask **apache2.socket**, **apache2.service**, and **nginx.service**:

```
# systemctl stop apache2.socket apache2.service nginx.service
# systemctl mask apache2.socket apache2.service nginx.service
```

Note: Other web server packages may exist. If not required and authorized by local site policy, they should also be removed. If the package is required for a dependency, the service and socket should be stopped and masked.

References:

1. NIST SP 800-53 Rev. 5: CM-7

Additional Information:

Several httpd servers exist and can use other service names. **apache2** and **nginx** are example services that provide an HTTP server. These and other services should also be audited

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software 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 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.1.19 Ensure xinetd services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The eXtended InterNET Daemon (**xinetd**) is an open source super daemon that replaced the original **inetd** daemon. The **xinetd** daemon listens for well known services and dispatches the appropriate daemon to properly respond to service requests.

Rationale:

If there are no **xinetd** services required, it is recommended that the package be removed to reduce the attack surface area of the system.

Note: If an **xinetd** service or services are required, ensure that any **xinetd** service not required is stopped and masked

Impact:

There may be packages that are dependent on the **xinetd** package. If the **xinetd** package is removed, these dependent packages will be removed as well. Before removing the **xinetd** package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask xinetd.service leaving the xinetd package installed.

Audit:

Run the following command to verify the **xinetd** package is not installed:

```
# dpkg-query -s xinetd &>/dev/null && echo "xinetd is installed"
```

Nothing should be returned.

-OR-

-IF- the **xinetd** package is required as a dependency:

Run the following command to verify **xinetd.service** is not enabled:

```
# systemctl is-enabled xinetd.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned

Run the following command to verify **xinetd.service** is not active:

```
# systemctl is-active xinetd.service 2>/dev/null | grep '^active'
```

Nothing should be returned

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop **xinetd.service**, and remove the **xinetd** package:

```
# systemctl stop xinetd.service  
# apt purge xinetd
```

-OR-

-IF- the **xinetd** package is required as a dependency:





Run the following commands to stop and mask the **xinetd.service**:

```
# systemctl stop xinetd.service  
# systemctl mask xinetd.service
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.1.20 Ensure X window server services are not in use (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The X Window System provides a Graphical User Interface (GUI) where users can have multiple windows in which to run programs and various add on. The X Windows system is typically used on workstations where users login, but not on servers where users typically do not login.

Rationale:

Unless your organization specifically requires graphical login access via X Windows, remove it to reduce the potential attack surface.

Impact:

If a Graphical Desktop Manager (GDM) is in use on the system, there may be a dependency on the **xorg-x11-server-common** package. If the GDM is required and approved by local site policy, the package should **not** be removed.

Many Linux systems run applications which require a Java runtime. Some Linux Java packages have a dependency on specific X Windows xorg-x11-fonts. One workaround to avoid this dependency is to use the "headless" Java packages for your specific Java runtime.

Audit:

- **IF** - a Graphical Desktop Manager or X-Windows server is not required and approved by local site policy:

Run the following command to Verify X Windows Server is not installed.

```
dpkg-query -s xserver-common &>/dev/null && echo "xserver-common is installed"
```

Nothing should be returned

Remediation:

- **IF** - a Graphical Desktop Manager or X-Windows server is not required and approved by local site policy:






Run the following command to remove the X Windows Server package:

```
# apt purge xserver-common
```

References:

1. NIST SP 800-53 Rev. 5: CM-11

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	2.6 <u>Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.1.21 Ensure mail transfer agent is configured for local-only mode (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Mail Transfer Agents (MTA), such as sendmail and Postfix, are used to listen for incoming mail and transfer the messages to the appropriate user or mail server. If the system is not intended to be a mail server, it is recommended that the MTA be configured to only process local mail.

Rationale:

The software for all Mail Transfer Agents is complex and most have a long history of security issues. While it is important to ensure that the system can process local mail messages, it is not necessary to have the MTA's daemon listening on a port unless the server is intended to be a mail server that receives and processes mail from other systems.

Run the following script to verify that the MTA is not listening on any non-loopback address (**127.0.0.1** or **::1**

```
#!/usr/bin/env bash

{
    a_output=(); a_output2=(); a_port_list=("25" "465" "587")
    for l_port_number in "${a_port_list[@]}"; do
        if ss -plntu | grep -P -- ':"$l_port_number"\b' | grep -Pvq --
'\h+(127\.0\.0\.1|\\[?::1\\]?):'"$l_port_number"'\b'; then
            a_output2+=(" - Port \"$l_port_number\" is listening on a non-
loopback network interface")
        else
            a_output+=(" - Port \"$l_port_number\" is not listening on a non-
loopback network interface")
        fi
    done
    if command -v postconf &> /dev/null; then
        l_interfaces="$(postconf -n inet_interfaces)"
    elif command -v exim &> /dev/null; then
        l_interfaces="$(exim -bP local_interfaces)"
    elif command -v sendmail &> /dev/null; then
        l_interfaces="$(grep -i "0 DaemonPortOptions=" /etc/mail/sendmail.cr |
grep -oP '?(=<Addr=)[^,]+')"
    fi
    if [ -n "$l_interfaces" ]; then
        if grep -Pqi '\ball\b' <<< "$l_interfaces"; then
            a_output2+=(" - MTA is bound to all network interfaces")
        elif ! grep -Pqi '(inet_interfaces\h*=\h*)?(0\.0\.0\.0|:::1|loopback-
only)' <<< "$l_interfaces"; then
            a_output2+=(" - MTA is bound to a network interface" "
\"$l_interfaces\"")
        else
            a_output+=(" - MTA is not bound to a non loopback network interface"
" \"$l_interfaces\"")
        fi
    else
        a_output+=(" - MTA not detected or in use")
    fi
    if [ "${#a_output2[@]}" -le 0 ]; then
        printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}"
    else
        printf '%s\n' "" "- Audit Result:" " ** FAIL **" " * Reasons for
audit failure *" "${a_output2[@]}" ""
        [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "- Correctly set:"
"${a_output[@]}"
    fi
}
}
```

Remediation:

Edit `/etc/postfix/main.cf` and add the following line to the RECEIVING MAIL section. If the line already exists, change it to look like the line below:

```
inet_interfaces = loopback-only
```

Run the following command to restart `postfix`:

```
# systemctl restart postfix
```

Note:

- This recommendation is designed around the postfix mail server.
- Depending on your environment you may have an alternative MTA installed such as exim4. If this is the case consult the documentation for your installed MTA to configure the recommended state.

References:

1. NIST SP 800-53 Rev. 5: CM-7

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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1018, T1018.000, T1210, T1210.000	TA0008	M1042

2.1.22 Ensure only approved services are listening on a network interface (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

A network port is identified by its number, the associated IP address, and the type of the communication protocol such as TCP or UDP.

A listening port is a network port on which an application or process listens on, acting as a communication endpoint.

Each listening port can be open or closed (filtered) using a firewall. In general terms, an open port is a network port that accepts incoming packets from remote locations.

Rationale:

Services listening on the system pose a potential risk as an attack vector. These services should be reviewed, and if not required, the service should be stopped, and the package containing the service should be removed. If required packages have a dependency, the service should be stopped and masked to reduce the attack surface of the system.

Impact:

There may be packages that are dependent on the service's package. If the service's package is removed, these dependent packages will be removed as well. Before removing the service's package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the `<service_name>.socket` and `<service_name>.service` leaving the service's package installed.

Audit:

Run the following command:

```
# ss -plntu
```

Review the output to ensure:

- All services listed are required on the system and approved by local site policy.
- Both the port and interface the service is listening on are approved by local site policy.
- If a listed service is not required:
 - Remove the package containing the service
 - **- IF -** the service's package is required for a dependency, stop and mask the service and/or socket

Remediation:

Run the following commands to stop the service and remove the package containing the service:

```
# systemctl stop <service_name>.socket <service_name>.service
# apt purge <package_name>
```

- OR - If required packages have a dependency:

Run the following commands to stop and mask the service and socket:

```
# systemctl stop <service_name>.socket <service_name>.service
# systemctl mask <service_name>.socket <service_name>.service
```

Note: replace **<service_name>** with the appropriate service name.

References:

1. NIST SP 800-53 Rev. 5: CM-7

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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2 Configure Client Services

A number of insecure services exist. While disabling the servers prevents a local attack against these services, it is advised to remove their clients unless they are required.

Note: This should not be considered a comprehensive list of insecure service clients. You may wish to consider additions to those listed here for your environment.

2.2.1 Ensure NIS Client is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Network Information Service (NIS), formerly known as Yellow Pages, is a client-server directory service protocol used to distribute system configuration files. The NIS client was used to bind a machine to an NIS server and receive the distributed configuration files.

Rationale:

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

Impact:

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

Audit:

Verify **nis** is not installed. Use the following command to provide the needed information:

```
# dpkg-query -s nis &>/dev/null && echo "nis is installed"
```

Nothing should be returned.

Remediation:






Uninstall **nis**:

```
# apt purge nis
```

References:

1. NIST SP 800-53 Rev. 5: CM-7, CM-11

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>2.6 Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1543, T1543.002	TA0008	M1042

2.2.2 Ensure rsh client is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The **rsh-client** package contains the client commands for the rsh services.

Rationale:

These legacy clients contain numerous security exposures and have been replaced with the more secure SSH package. Even if the server is removed, it is best to ensure the clients are also removed to prevent users from inadvertently attempting to use these commands and therefore exposing their credentials. Note that removing the **rsh-client** package removes the clients for **rsh**, **rcp** and **rlogin**.

Impact:

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

Audit:

Verify **rsh-client** is not installed. Use the following command to provide the needed information:

```
# dpkg-query -s rsh-client &>/dev/null && echo "rsh-client is installed"
```

Nothing should be returned.

Remediation:





Uninstall **rsh**:

```
# apt purge rsh-client
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1040, T1040.000, T1203, T1203.000, T1543, T1543.002	TA0008	M1041, M1042

2.2.3 Ensure talk client is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The **talk** software makes it possible for users to send and receive messages across systems through a terminal session. The **talk** client, which allows initialization of talk sessions, is installed by default.

Rationale:

The software presents a security risk as it uses unencrypted protocols for communication.

Impact:

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

Audit:

Verify **talk** is not installed. The following command may provide the needed information:

```
# dpkg-query -s talk &>/dev/null && echo "talk is installed"
```

Nothing should be returned.

Remediation:





Uninstall **talk**:

```
# apt purge talk
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1543, T1543.002	TA0006, TA0008	M1041, M1042

2.2.4 Ensure telnet client is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `inetutils-telnet` package contains the `telnet` client, which allows users to start connections to other systems via the telnet protocol.

Rationale:

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

Impact:

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

Audit:

Verify `inetutils-telnet` & `telnet` are not installed. Use the following command to provide the needed information:

```
# dpkg-query -f='${Package} ${Version} ${Architecture}\n' -W inetutils-telnet telnet >/dev/null && echo "telnet is installed"
```

Nothing should be returned.

Remediation:





Run the following commands to uninstall `telnet` & `inetutils-telnet`:

```
# apt purge telnet
# apt purge inetutils-telnet
```

References:

1. NIST SP 800-53 Rev. 5: CM-7, CM-11

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1040, T1040.000, T1203, T1203.000, T1543, T1543.002	TA0006, TA0008	M1041, M1042

2.2.5 Ensure ldap client is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Lightweight Directory Access Protocol (LDAP) was introduced as a replacement for NIS/YP. It is a service that provides a method for looking up information from a central database.

Rationale:

If the system will not need to act as an LDAP client, it is recommended that the software be removed to reduce the potential attack surface.

Impact:

Removing the LDAP client will prevent or inhibit using LDAP for authentication in your environment.

Audit:

Verify that **ldap-utils** is not installed. Use the following command to provide the needed information:

```
# dpkg-query -s ldap-utils &>/dev/null && echo "ldap-utils is installed"
```

Nothing should be returned.

Remediation:





Uninstall **ldap-utils**:

```
# apt purge ldap-utils
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1543, T1543.002	TA0008	M1042

2.2.6 Ensure *ftp* client is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

tnftp an enhanced FTP client, is the user interface to the Internet standard File Transfer Protocol. The program allows a user to transfer files to and from a remote network site.

Rationale:

Unless there is a need to run the system using Internet standard File Transfer Protocol (for example, to allow anonymous downloads), it is recommended that the package be removed to reduce the potential attack surface.

Audit:

Verify **tnftp** & **ftp** is not installed. Use the following command to provide the needed information:

```
# dpkg-query -l | grep -E 'ftp|tnftp' &>/dev/null && echo "ftp is installed"
```

Nothing should be returned.

Remediation:





Run the following commands to uninstall **tnftp** & **ftp**:

```
# apt purge ftp
# apt purge tnftp
```

References:

1. NIST SP 800-53 Rev. 5: CM-7, CM-11

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1543, T1543.002	TA0008	M1042

2.3 Configure Time Synchronization

It is recommended that systems be configured to synchronize their time using a service such as `systemd-timesyncd`, or `chrony`.

Virtual systems may be configured to receive their time synchronization from their host system.

The host system must be configured to synchronize its time from an authoritative source to be considered compliant with this section.

Any "physical" clock present on a system should be synchronized from an authoritative time source.

Only one time synchronization method should be in use on the system

Notes: Only the section related to the time synchronization method in use on the system should be followed, all other time synchronization recommendations should be skipped

2.3.1 Ensure time synchronization is in use

It is recommended that physical systems and virtual guests lacking direct access to the physical host's clock be configured to synchronize their time using a service such as `systemd-timesyncd`, or `chrony`.

2.3.1.1 Ensure a single time synchronization daemon is in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

System time should be synchronized between all systems in an environment. This is typically done by establishing an authoritative time server or set of servers and having all systems synchronize their clocks to them.

Note:

- **On virtual systems where host based time synchronization is available consult your virtualization software documentation and verify that host based synchronization is in use and follows local site policy. In this scenario, this section should be skipped**
- Only **one** time synchronization method should be in use on the system. Configuring multiple time synchronization methods could lead to unexpected or unreliable results

Rationale:

Time synchronization is important to support time sensitive security mechanisms and ensures log files have consistent time records across the enterprise, which aids in forensic investigations.

Audit:

On physical systems, and virtual systems where host based time synchronization is not available.

One of the two time synchronization daemons should be available; **chrony** or **systemd-timesyncd**

Run the following script to verify that a single time synchronization daemon is available on the system:

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    service_not_enabled_chk()
    {
        l_out2=""
        if systemctl is-enabled "$l_service_name" 2>/dev/null | grep -q 'enabled'; then
            l_out2="$l_out2\n - Daemon: \"$l_service_name\" is enabled on the system"
        fi
        if systemctl is-active "$l_service_name" 2>/dev/null | grep -q '^active'; then
            l_out2="$l_out2\n - Daemon: \"$l_service_name\" is active on the system"
        fi
    }
    l_service_name="systemd-timesyncd.service" # Check systemd-timesyncd daemon
    service_not_enabled_chk
    if [ -n "$l_out2" ]; then
        l_timesyncd="y"
        l_out_tsd="$l_out2"
    else
        l_timesyncd="n"
        l_out_tsd="\n - Daemon: \"$l_service_name\" is not enabled and not active on the system"
    fi
    l_service_name="chrony.service" # Check chrony
    service_not_enabled_chk
    if [ -n "$l_out2" ]; then
        l_chrony="y"
        l_out_chrony="$l_out2"
    else
        l_chrony="n"
        l_out_chrony="\n - Daemon: \"$l_service_name\" is not enabled and not active on the
system"
    fi
    l_status="$l_timesyncd$l_chrony"
    case "$l_status" in
        yy)
            l_output2=" - More than one time sync daemon is in use on the
system$l_out_tsd$l_out_chrony"
            ;;
        nn)
            l_output2=" - No time sync daemon is in use on the system$l_out_tsd$l_out_chrony"
            ;;
        yn|ny)
            l_output=" - Only one time sync daemon is in use on the
system$l_out_tsd$l_out_chrony"
            ;;
        *)
            l_output2=" - Unable to determine time sync daemon(s) status"
            ;;
    esac

    if [ -z "$l_output2" ]; then
        echo -e "\n- Audit Result:\n ** PASS **\n$l_output\n"
    else
        echo -e "\n- Audit Result:\n ** FAIL **\n - * Reasons for audit failure *
:\n$l_output2\n"
    fi
}

```

Note: Follow the guidance in the subsection for the time synchronization daemon available on the system and skip the other time synchronization daemon subsection.

Remediation:

On physical systems, and virtual systems where host based time synchronization is not available.

Select **one** of the two time synchronization daemons; **chrony (1)** or **systemd-timesyncd (2)** and following the remediation procedure for the selected daemon.

Note: enabling more than one synchronization daemon could lead to unexpected or unreliable results:

1. **chrony**

Run the following command to install **chrony**:

```
# apt install chrony
```

Run the following commands to stop and mask the **systemd-timesyncd** daemon:

```
# systemctl stop systemd-timesyncd.service
# systemctl mask systemd-timesyncd.service
```

Note:

- Subsection: **Configure chrony** should be followed
- Subsection: **Configure systemd-timesyncd** should be skipped

2. **systemd-timesyncd**

Run the following command to remove the chrony package:

```
# apt purge chrony
# apt autoremove chrony
```





Note:

- Subsection: **Configure systemd-timesyncd** should be followed
- Subsection: **Configure chrony** should be skipped

References:

1. NIST SP 800-53 Rev. 5: AU-3, AU-12

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.001	TA0005	

2.3.2 Configure systemd-timesyncd

systemd-timesyncd is a daemon that has been added for synchronizing the system clock across the network. It implements an SNTP client. In contrast to NTP implementations such as chrony or the NTP reference server this only implements a client side, and does not bother with the full NTP complexity, focusing only on querying time from one remote server and synchronizing the local clock to it. The daemon runs with minimal privileges, and has been hooked up with networkd to only operate when network connectivity is available. The daemon saves the current clock to disk every time a new NTP sync has been acquired, and uses this to possibly correct the system clock early at bootup, in order to accommodate for systems that lack an RTC such as the Raspberry Pi and embedded devices, and make sure that time monotonically progresses on these systems, even if it is not always correct. To make use of this daemon a new system user and group "systemd-timesync" needs to be created on installation of systemd.

The default configuration is set during compilation, so configuration is only needed when it is necessary to deviate from those defaults. Initially, the main configuration file in `/etc/systemd/` contains commented out entries showing the defaults as a guide to the administrator. Local overrides can be created by editing this file or by creating drop-ins, as described below. Using drop-ins for local configuration is recommended over modifications to the main configuration file.

In addition to the "main" configuration file, drop-in configuration snippets are read from `/usr/lib/systemd/*.conf.d/`, `/usr/local/lib/systemd/*.conf.d/`, and `/etc/systemd/*.conf.d/`. Those drop-ins have higher precedence and override the main configuration file. Files in the `*.conf.d/` configuration subdirectories are sorted by their filename in lexicographic order, regardless of in which of the subdirectories they reside. When multiple files specify the same option, for options which accept just a single value, the entry in the file sorted last takes precedence, and for options which accept a list of values, entries are collected as they occur in the sorted files.

When packages need to customize the configuration, they can install drop-ins under `/usr/`. Files in `/etc/` are reserved for the local administrator, who may use this logic to override the configuration files installed by vendor packages. Drop-ins have to be used to override package drop-ins, since the main configuration file has lower precedence. It is recommended to prefix all filenames in those subdirectories with a two-digit number and a dash, to simplify the ordering of the files.

To disable a configuration file supplied by the vendor, the recommended way is to place a symlink to `/dev/null` in the configuration directory in `/etc/`, with the same filename as the vendor configuration file.

Note:

- The recommendations in this section only apply if **timesyncd** is in use on the system
- The **systemd-timesyncd** service specifically implements only SNTP.
 - This minimalistic service will set the system clock for large offsets or slowly adjust it for smaller deltas
 - More complex use cases are not covered by **systemd-timesyncd**
- **If chrony is used, systemd-timesyncd should be stopped and masked, and this section skipped**
- **One, and only one, time synchronization method should be in use on the system**

2.3.2.1 Ensure systemd-timesyncd configured with authorized timeserver (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

NTP=

- A space-separated list of NTP server host names or IP addresses. During runtime this list is combined with any per-interface NTP servers acquired from systemd-networkd.service(8). systemd-timesyncd will contact all configured system or per-interface servers in turn, until one responds. When the empty string is assigned, the list of NTP servers is reset, and all prior assignments will have no effect. This setting defaults to an empty list.

FallbackNTP=

- A space-separated list of NTP server host names or IP addresses to be used as the fallback NTP servers. Any per-interface NTP servers obtained from systemd-networkd.service(8) take precedence over this setting, as do any servers set via NTP= above. This setting is hence only relevant if no other NTP server information is known. When the empty string is assigned, the list of NTP servers is reset, and all prior assignments will have no effect. If this option is not given, a compiled-in list of NTP servers is used.

Rationale:

Time synchronization is important to support time sensitive security mechanisms and to ensure log files have consistent time records across the enterprise to aid in forensic investigations

Audit:

Run the following command to verify the **NTP** and/or **FallbackNTP** option is set to local site approved authoritative time server(s):

```

#!/usr/bin/env bash

{
  a_output=(); a_output2=(); a_parlist=("NTP=[^#\n\r]+" "FallbackNTP=[^#\n\r]+")
  l_systemd_config_file="/etc/systemd/timesyncd.conf" # Main systemd configuration file
  f_config_file_parameter_chk()
  {
    unset A_out; declare -A A_out # Check config file(s) setting
    while read -r l_out; do
      if [ -n "$l_out" ]; then
        if [[ $l_out =~ ^\s*# ]]; then
          l_file="$l_out// # /"
        else
          l_systemd_parameter="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
          grep -Piq -- "\h*$l_systemd_parameter_name\b" <<< "$l_systemd_parameter" &&
          A_out+=(["$l_systemd_parameter"]="$l_file")
        fi
      fi
    done < <("$l_systemdanalyze" cat-config "$l_systemd_config_file" | grep -Pio
    '\h*([^\h*\n\r]+|\h*\h*\/[^\h*\n\r\h]+\h*\h*\b)')
    if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate output
      while IFS="" read -r l_systemd_file_parameter_name l_systemd_file_parameter_value; do
        l_systemd_file_parameter_name="${l_systemd_file_parameter_name// /}"
        l_systemd_file_parameter_value="${l_systemd_file_parameter_value// /}"
        if grep -Piq "\b$l_systemd_file_parameter_name\b" <<< "$l_systemd_file_parameter_value";
      then
        a_output+=(" - \"$l_systemd_file_parameter_name\" is correctly set to
        \"$l_systemd_file_parameter_value\"
        " in \"$(printf '%s' "${A_out[@]}")\"")
      else
        a_output2+=(" - \"$l_systemd_file_parameter_name\" is incorrectly set to
        \"$l_systemd_file_parameter_value\"
        " in \"$(printf '%s' "${A_out[@]}")\" and should have a value matching:
        \"$l_value_out\"")
      fi
      done < <(grep -Pio -- "\h*$l_systemd_file_parameter_name\b\h*\h*\h*" "${A_out[@]}")
    else
      a_output2+=(" - \"$l_systemd_file_parameter_name\" is not set in an included file \"
      \" *** Note: \"$l_systemd_file_parameter_name\" May be set in a file that's ignored by load
      procedure ***")
    fi
  }
  l_systemdanalyze="$(readlink -f /bin/systemd-analyze)"
  while IFS="" read -r l_systemd_parameter_name l_systemd_parameter_value; do # Assess and
  check parameters
    l_systemd_parameter_name="${l_systemd_parameter_name// /}";
    l_systemd_parameter_value="${l_systemd_parameter_value// /}"
    l_value_out="${l_systemd_parameter_value//-/ through }"; l_value_out="${l_value_out// or
    }"
    l_value_out="$(tr -d '()' <<< "$l_value_out")"
    f_config_file_parameter_chk
    done < <(printf '%s\n' "${a_parlist[@]}")
    if [ "${#a_output2[@]}" -le 0 ]; then
      printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
    else
      printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for audit failure:"
      "${a_output2[@]}"
      [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "" "- Correctly set:" "${a_output[@]}" ""
    fi
  }
}

```

Example output:


```
- Audit Result:
  ** PASS **
- "NTP" is correctly set to "time.nist.gov"
  in "/etc/systemd/timesyncd.conf.d/60-timesyncd.conf"
- "FallbackNTP" is correctly set to "time-a-g.nist.gov"
  in "/etc/systemd/timesyncd.conf.d/60-timesyncd.conf"
```

Note: Please ensure the output for **NTP** and/or **FallbackNTP** is in accordance with local site policy. The timeservers in the example output are provided as an example of possible timeservers and they may not follow local site policy.

Remediation:

Set **NTP** and/or **FallbackNTP** parameters to local site approved authoritative time server(s) in `/etc/systemd/timesyncd.conf` or a file in `/etc/systemd/timesyncd.conf.d/` ending in `.conf` in the **[Time]** section:

Example file:

```
[Time]
NTP=time.nist.gov # Uses the generic name for NIST's time servers
FallbackNTP=time-a-g.nist.gov time-b-g.nist.gov time-c-g.nist.gov # Space
separated list of NIST time servers
```

Example script to create systemd drop-in configuration file:

```
#!/usr/bin/env bash

{
    a_settings=("NTP=time.nist.gov" "FallbackNTP=time-a-g.nist.gov time-b-
g.nist.gov time-c-g.nist.gov")
    [ ! -d /etc/systemd/timesyncd.conf.d/ ] && mkdir
/etc/systemd/timesyncd.conf.d/
    if grep -Psq -- '^\h*\[Time\]' /etc/systemd/timesyncd.conf.d/60-
timesyncd.conf; then
        printf '%s\n' "" "${a_settings[@]}" >>
/etc/systemd/timesyncd.conf.d/60-timesyncd.conf
    else
        printf '%s\n' "" "[Time]" "${a_settings[@]}" >>
/etc/systemd/timesyncd.conf.d/60-timesyncd.conf
    fi
}
```

Note: If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten

Run the following command to update the parameters in the service:

```
# systemctl reload-or-restart systemd-journald
```

Default Value:





#NTP=

#FallbackNTP=

References:

1. <https://www.freedesktop.org/software/systemd/man/timesyncd.conf.html>
2. <https://tf.nist.gov/tf-cgi/servers.cgi>
3. NIST SP 800-53 Rev. 5: AU-7, AU-8

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.001	TA0002	M1022

2.3.2.2 Ensure systemd-timesyncd is enabled and running (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

systemd-timesyncd is a daemon that has been added for synchronizing the system clock across the network

Rationale:

systemd-timesyncd needs to be enabled and running in order to synchronize the system to a timeserver.

Time synchronization is important to support time sensitive security mechanisms and to ensure log files have consistent time records across the enterprise to aid in forensic investigations

Audit:

- **IF** - systemd-timesyncd is in use on the system, run the following commands:
Run the following command to verify that the **systemd-timesyncd** service is enabled:

```
# systemctl is-enabled systemd-timesyncd.service  
  
enabled
```

Run the following command to verify that the **systemd-timesyncd** service is active:

```
# systemctl is-active systemd-timesyncd.service  
  
active
```

Remediation:

- IF - **systemd-timesyncd** is in use on the system, run the following commands:
Run the following command to unmask **systemd-timesyncd.service**:

```
# systemctl unmask systemd-timesyncd.service
```

Run the following command to enable and start **systemd-timesyncd.service**:

```
# systemctl --now enable systemd-timesyncd.service
```

- OR -





If another time synchronization service is in use on the system, run the following command to stop and mask **systemd-timesyncd**:

```
# systemctl --now mask systemd-timesyncd.service
```

References:

1. NIST SP 800-53 Rev. 5: AU-7, AU-8

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.001	TA0002	M1022

2.3.3 Configure chrony

chrony is a daemon which implements the Network Time Protocol (NTP) and is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate.

chrony can be configured to be a client and/or a server.

More information on **chrony** can be found at: <http://chrony.tuxfamily.org/>.

Note:

- If **systemd-timesyncd** is being used, **chrony** should be removed and this section skipped
- Only one time synchronization method should be in use on the system

2.3.3.1 Ensure chrony is configured with authorized timeserver (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

- server
 - The server directive specifies an NTP server which can be used as a time source. The client-server relationship is strictly hierarchical: a client might synchronize its system time to that of the server, but the server's system time will never be influenced by that of a client.
 - This directive can be used multiple times to specify multiple servers.
 - The directive is immediately followed by either the name of the server, or its IP address.
- pool
 - The syntax of this directive is similar to that for the server directive, except that it is used to specify a pool of NTP servers rather than a single NTP server. The pool name is expected to resolve to multiple addresses which might change over time.
 - This directive can be used multiple times to specify multiple pools.
 - All options valid in the server directive can be used in this directive too.

Rationale:

Time synchronization is important to support time sensitive security mechanisms and to ensure log files have consistent time records across the enterprise to aid in forensic investigations

Audit:

- IF - **chrony** is in use on the system, run the following script to ensure **chrony** is configured with an authorized timeserver:

```
#!/usr/bin/env bash

{
    a_output=() a_output2=() a_config_files=("/etc/chrony/chrony.conf")
    l_include='(confdir|sourcedir)' l_parameter_name='(server|pool)'
    l_parameter_value='.'
    while IFS= read -r l_conf_loc; do
        l_dir="" l_ext=""
        if [ -d "$l_conf_loc" ]; then
            l_dir="$l_conf_loc" l_ext=""
        elif grep -Psq '\/*\.[^\#/\n\r+]?h*$' <<< "$l_conf_loc" || [ -f
"$$(readlink -f "$l_conf_loc")" ]; then
            l_dir="$(dirname "$l_conf_loc")" l_ext="$(basename "$l_conf_loc")"
        fi
        if [[ -n "$l_dir" && -n "$l_ext" ]]; then
            while IFS= read -r -d $'\0' l_file_name; do
                [ -f "$(readlink -f "$l_file_name")" ] &&
a_config_files+=("$$(readlink -f "$l_file_name")")
                done < <(find -L "$l_dir" -type f -name "$l_ext" -print0
2>/dev/null)
            fi
            done < <(awk 'l~/^s*'"$l_include"'${print $2}' "${a_config_files[*]}"
2>/dev/null)
            for l_file in "${a_config_files[@]"; do
                l_parameter_line="$(grep -Psi
'^h*'"$l_parameter_name"'(\h+|\h*:\h*)'"$l_parameter_value"'b' "$l_file")"
                [ -n "$l_parameter_line" ] && a_output+=(" - Parameter: \"$(tr -d '()'
<<< ${l_parameter_name//|/ or })\" \" \"
                    "      Exists in the file: \"$l_file\" as: \" $l_parameter_line")
            done
            [ "${#a_output[@]}" -le 0 ] && a_output2+=(" - Parameter: \"$(tr -d
'()' <<< ${l_parameter_name//|/ or })\" \" \"
                "      Does not exist in the chrony configuration")
            if [ "${#a_output2[@]}" -le 0 ]; then
                printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
            else
                printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
            fi
        fi
    }
}
```

Remediation:

Edit `/etc/chrony/chrony.conf` or a file ending in `.sources` in `/etc/chrony/sources.d/` and add or edit server or pool lines as appropriate according to local site policy:

Edit the **Chrony** configuration and add or edit the server and/or pool lines returned by the Audit Procedure as appropriate according to local site policy

```
<[server|pool]> <[remote-server|remote-pool]>
```

*Example script to add a drop-in configuration for the **pool** directive:*

```
#!/usr/bin/env bash

{
    [ ! -d "/etc/chrony/sources.d/" ] && mkdir /etc/chrony/sources.d/
    printf '%s\n' "" "#The maxsources option is unique to the pool directive"
    \
    "pool time.nist.gov iburst maxsources 4" >> /etc/chrony/sources.d/60-
sources.sources
    chronyc reload sources &>/dev/null
}
```

*Example script to add a drop-in configuration for the **server** directive:*

```
#!/usr/bin/env bash

{
    [ ! -d "/etc/chrony/sources.d/" ] && mkdir /etc/chrony/sources.d/
    printf '%s\n' "" "server time-a-g.nist.gov iburst" "server 132.163.97.3
iburst" \
    "server time-d-b.nist.gov iburst" >> /etc/chrony/sources.d/60-
sources.sources
    chronyc reload sources &>/dev/null
}
```

Run the following command to reload the **chronyd** config:

```
# systemctl reload-or-restart chronyd
```

References:

1. `chrony.conf(5)` Manual Page
2. <https://tf.nist.gov/tf-cgi/servers.cgi>
3. NIST SP 800-53 Rev. 5: AU-3, AU-12

Additional Information:

If pool and/or server directive(s) are set in a sources file in `/etc/chrony/sources.d`, the line:

```
sourcedir /etc/chrony/sources.d
```

must be present in `/etc/chrony/chrony.conf`

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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.001	TA0002	M1022

2.3.3.2 Ensure chrony is running as user _chrony (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The **chrony** package is installed with a dedicated user account **_chrony**. This account is granted the access required by the **chronyd** service

Rationale:

The **chronyd** service should run with only the required privildges

Audit:

- **IF** - **chrony** is in use on the system, run the following command to verify the **chronyd** service is being run as the **_chrony** user:

```
# ps -ef | awk '(/[c]hronyd/ && $1!="_chrony") { print $1 }'
```

Nothing should be returned

Remediation:

Add or edit the **user** line to **/etc/chrony/chrony.conf** or a file ending in **.conf** in **/etc/chrony/conf.d/**:

```
user _chrony
```

- OR -

If another time synchronization service is in use on the system, run the following command to remove **chrony** from the system:

```
# apt purge chrony
# apt autoremove chrony
```

Default Value:

user _chrony

References:

1. NIST SP 800-53 Rev. 5: AU-8

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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.001	TA0002	M1022

2.3.3.3 Ensure chrony is enabled and running (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

chrony is a daemon for synchronizing the system clock across the network

Rationale:

chrony needs to be enabled and running in order to synchronize the system to a timeserver.

Time synchronization is important to support time sensitive security mechanisms and to ensure log files have consistent time records across the enterprise to aid in forensic investigations

Audit:

- **IF** - chrony is in use on the system, run the following commands:
Run the following command to verify that the **chrony** service is enabled:

```
# systemctl is-enabled chrony.service  
enabled
```

Run the following command to verify that the **chrony** service is active:

```
# systemctl is-active chrony.service  
active
```

Remediation:

- IF - **chrony** is in use on the system, run the following commands:
Run the following command to unmask **chrony.service**:

```
# systemctl unmask chrony.service
```

Run the following command to enable and start **chrony.service**:

```
# systemctl --now enable chrony.service
```

- OR -

If another time synchronization service is in use on the system, run the following command to remove **chrony**:

```
# apt purge chrony
# apt autoremove chrony
```

References:

1. NIST SP 800-53 Rev. 5: AU-8

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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.001	TA0002	M1022

2.4 Job Schedulers

A job scheduler is used to execute jobs, commands, or shell scripts, at fixed times, dates, or intervals

2.4.1 Configure cron

cron is a time based job scheduler

- **IF** - **cron** is not installed on the system, this sub section can be skipped

Note: Other methods such as **systemd timers** exist for scheduling jobs. If another method is used **cron** should may be removed. The alternate method should be secured in accordance with local site policy

2.4.1.1 Ensure cron daemon is enabled and active (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The **cron** daemon is used to execute batch jobs on the system.

Rationale:

While there may not be user jobs that need to be run on the system, the system does have maintenance jobs that may include security monitoring that have to run, and **cron** is used to execute them.

Audit:

- **IF** - cron is installed on the system:

Run the following command to verify **cron** is enabled:

```
# systemctl list-unit-files | awk '$1~/^crond?\.service/{print $2}'  
  
enabled
```

Run the following command to verify that **cron** is active:

```
# systemctl list-units | awk '$1~/^crond?\.service/{print $3}'  
  
active
```

Remediation:

- **IF** - cron is installed on the system:

Run the following commands to unmask, enable, and start **cron**:

```
# systemctl unmask "$(systemctl list-unit-files | awk  
'$1~/^crond?\.service/{print $1}')" "  
# systemctl --now enable "$(systemctl list-unit-files | awk  
'$1~/^crond?\.service/{print $1}')" "
```

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.001	TA0005	M1018

2.4.1.2 Ensure permissions on /etc/crontab are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/crontab` file is used by `cron` to control its own jobs. The commands in this item make sure that root is the user and group owner of the file and that only the owner can access the file.

Rationale:

This file contains information on what system jobs are run by cron. Write access to these files could provide unprivileged users with the ability to elevate their privileges. Read access to these files could provide users with the ability to gain insight on system jobs that run on the system and could provide them a way to gain unauthorized privileged access.

Audit:

- **IF** - cron is installed on the system:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other` :

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/crontab
Access: (600/-rw-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

- **IF** - cron is installed on the system:

Run the following commands to set ownership and permissions on `/etc/crontab`:

```
# chown root:root /etc/crontab
# chmod og-rwx /etc/crontab
```

Default Value:

Access: (644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002, TA0007	M1018

2.4.1.3 Ensure permissions on /etc/cron.hourly are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

This directory contains system **cron** jobs that need to run on an hourly basis. The files in this directory cannot be manipulated by the **crontab** command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

- **IF** - cron is installed on the system:

Run the following command and verify **Uid** and **Gid** are both **0/root** and **Access** does not grant permissions to **group** or **other**:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.hourly/  
Access: (700/drwx-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

- **IF** - cron is installed on the system:

Run the following commands to set ownership and permissions on the **/etc/cron.hourly** directory:

```
# chown root:root /etc/cron.hourly/  
# chmod og-rwx /etc/cron.hourly/
```







Default Value:

Access: (755/drwxr-xr-x) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002, TA0007	M1018

2.4.1.4 Ensure permissions on /etc/cron.daily are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/cron.daily` directory contains system cron jobs that need to run on a daily basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

- **IF** - cron is installed on the system:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.daily/  
Access: (700/drwx-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

- **IF** - cron is installed on the system:

Run the following commands to set ownership and permissions on the `/etc/cron.daily` directory:

```
# chown root:root /etc/cron.daily/  
# chmod og-rwx /etc/cron.daily/
```







Default Value:

Access: (755/drwxr-xr-x) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002, TA0007	M1018

2.4.1.5 Ensure permissions on /etc/cron.weekly are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/cron.weekly` directory contains system cron jobs that need to run on a weekly basis. The files in this directory cannot be manipulated by the `crontab` command but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

- **IF** - cron is installed on the system:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.weekly/  
Access: (700/drwx-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

- **IF** - cron is installed on the system:

Run the following commands to set ownership and permissions on the `/etc/cron.weekly` directory:

```
# chown root:root /etc/cron.weekly/  
# chmod og-rwx /etc/cron.weekly/
```







Default Value:

Access: (755/drwxr-xr-x) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002, TA0007	M1018

2.4.1.6 Ensure permissions on /etc/cron.monthly are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/cron.monthly` directory contains system cron jobs that need to run on a monthly basis. The files in this directory cannot be manipulated by the `crontab` command but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

- **IF** - cron is installed on the system:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.monthly/  
Access: (700/drwx-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

- **IF** - cron is installed on the system:

Run the following commands to set ownership and permissions on the `/etc/cron.monthly` directory:

```
# chown root:root /etc/cron.monthly/  
# chmod og-rwx /etc/cron.monthly/
```

Default Value:

Access: (755/drwxr-xr-x) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002, TA0007	M1018

2.4.1.7 Ensure permissions on /etc/cron.d are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/cron.d` directory contains system `cron` jobs that need to run in a similar manner to the hourly, daily weekly and monthly jobs from `/etc/crontab`, but require more granular control as to when they run. The files in this directory cannot be manipulated by the `crontab` command but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

- **IF** - cron is installed on the system:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.d/  
Access: (700/drwx-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

- **IF** - cron is installed on the system:

Run the following commands to set ownership and permissions on the `/etc/cron.d` directory:

```
# chown root:root /etc/cron.d/  
# chmod og-rwx /etc/cron.d/
```







Default Value:

Access: (755/drwxr-xr-x) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002, TA0007	M1018

2.4.1.8 Ensure crontab is restricted to authorized users (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

crontab is the program used to install, deinstall, or list the tables used to drive the cron daemon. Each user can have their own crontab, and though these are files in **/var/spool/cron/crontabs**, they are not intended to be edited directly.

If the **/etc/cron.allow** file exists, then you must be listed (one user per line) therein in order to be allowed to use this command. If the **/etc/cron.allow** file does not exist but the **/etc/cron.deny** file does exist, then you must not be listed in the **/etc/cron.deny** file in order to use this command.

If neither of these files exists, then depending on site-dependent configuration parameters, only the super user will be allowed to use this command, or all users will be able to use this command.

If both files exist then **/etc/cron.allow** takes precedence. Which means that **/etc/cron.deny** is not considered and your user must be listed in **/etc/cron.allow** in order to be able to use the crontab.

Regardless of the existence of any of these files, the root administrative user is always allowed to setup a crontab.

The files **/etc/cron.allow** and **/etc/cron.deny**, if they exist, must be either world-readable, or readable by group **crontab**. If they are not, then cron will deny access to all users until the permissions are fixed.

There is one file for each user's crontab under the **/var/spool/cron/crontabs** directory. Users are not allowed to edit the files under that directory directly to ensure that only users allowed by the system to run periodic tasks can add them, and only syntactically correct crontabs will be written there. This is enforced by having the directory writable only by the **crontab** group and configuring crontab command with the setgid bit set for that specific group.

Note:

- Even though a given user is not listed in **cron.allow**, cron jobs can still be run as that user
- The files **/etc/cron.allow** and **/etc/cron.deny**, if they exist, only controls administrative access to the crontab command for scheduling and modifying cron jobs

Rationale:

On many systems, only the system administrator is authorized to schedule **cron** jobs. Using the **cron.allow** file to control who can run **cron** jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

Audit:

- **IF** - cron is installed on the system:

Run the following command to verify **/etc/cron.allow**:

- Exists
- Is mode **0640** or more restrictive
- Is owned by the user **root**
- Is group owned by the group **root** - **OR** - the group **crontab**

```
# stat -Lc 'Access: (%a/%A) Owner: (%U) Group: (%G)' /etc/cron.allow
```

Verify the returned value is:

```
Access: (640/-rw-r-----) Owner: (root) Group: (root)
- OR -
Access: (640/-rw-r-----) Owner: (root) Group: (crontab)
```

Run the following command to verify either **cron.deny** doesn't exist or is:

- Mode **0640** or more restrictive
- Owned by the user **root**
- Is group owned by the group **root** - **OR** - the group **crontab**

```
# [ -e "/etc/cron.deny" ] && stat -Lc 'Access: (%a/%A) Owner: (%U) Group: (%G)' /etc/cron.deny
```

Verify either nothing is returned - **OR** - returned value is one of the following:

```
Access: (640/-rw-r-----) Owner: (root) Group: (root)
- OR -
Access: (640/-rw-r-----) Owner: (root) Group: (crontab)
```

Note: On systems where cron is configured to use the group **crontab**, if the group **crontab** is not set as the owner of **cron.allow**, then cron will deny access to all users and you will see an error similar to:

```
You (<USERNAME>) are not allowed to use this program (crontab)
See crontab(1) for more information
```

Remediation:

- **IF** - cron is installed on the system:

Run the following script to:

- Create `/etc/cron.allow` if it doesn't exist
- Change owner to user `root`
- Change group owner to group `root` - **OR** - group `crontab` if it exists
- Change mode to `640` or more restrictive

```
#!/usr/bin/env bash

{
  [ ! -e "/etc/cron.allow" ] && touch /etc/cron.allow
  chmod u-x,g-wx,o-rwx /etc/cron.allow
  if grep -Pq -- '^\h*crontab\: ' /etc/group; then
    chown root:crontab /etc/cron.allow
  else
    chown root:root /etc/cron.allow
  fi
}
```

- **IF** - `/etc/cron.deny` exists, run the following script to:

- Change owner to user `root`
- Change group owner to group `root` - **OR** - group `crontab` if it exists
- Change mode to `640` or more restrictive

```
#!/usr/bin/env bash

{
  if [ -e "/etc/cron.deny" ]; then
    chmod u-x,g-wx,o-rwx /etc/cron.deny
    if grep -Pq -- '^\h*crontab\: ' /etc/group; then
      chown root:crontab /etc/cron.deny
    else
      chown root:root /etc/cron.deny
    fi
  fi
}
```







Note: On systems where cron is configured to use the group `crontab`, if the group `crontab` is not set as the owner of `cron.allow`, then cron will deny access to all users and you will see an error similar to:

```
You (<USERNAME>) are not allowed to use this program (crontab)
See crontab(1) for more information
```

References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002	M1018

2.4.2 Configure at

at is a command-line utility used to schedule a job for later execution

Note: if **at** is not installed on the system, this section can be skipped

2.4.2.1 Ensure at is restricted to authorized users (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

at allows fairly complex time specifications, extending the POSIX.2 standard. It accepts times of the form HH:MM to run a job at a specific time of day. (If that time is already past, the next day is assumed.) You may also specify midnight, noon, or teatime (4pm) and you can have a time-of-day suffixed with AM or PM for running in the morning or the evening. You can also say what day the job will be run, by giving a date in the form month-name day with an optional year, or giving a date of the form MMDD[CC]YY, MM/DD/[CC]YY, DD.MM.[CC]YY or [CC]YY-MM-DD. The specification of a date must follow the specification of the time of day. You can also give times like now + count time-units, where the time-units can be minutes, hours, days, or weeks and you can tell at to run the job today by suffixing the time with today and to run the job tomorrow by suffixing the time with tomorrow.

The **/etc/at.allow** and **/etc/at.deny** files determine which user can submit commands for later execution via at or batch. The format of the files is a list of usernames, one on each line. Whitespace is not permitted. If the file **/etc/at.allow** exists, only usernames mentioned in it are allowed to use at. If **/etc/at.allow** does not exist, **/etc/at.deny** is checked, every username not mentioned in it is then allowed to use at. An empty **/etc/at.deny** means that every user may use at. If neither file exists, only the superuser is allowed to use at.

Rationale:

On many systems, only the system administrator is authorized to schedule **at** jobs. Using the **at.allow** file to control who can run **at** jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

Audit:

- **IF** - at is installed on the system:

Run the following command to verify `/etc/at.allow`:

- Exists
- Is mode `0640` or more restrictive
- Is owned by the user `root`
- Is group owned by the group `daemon` or group `root`

```
# stat -Lc 'Access: (%a/%A) Owner: (%U) Group: (%G)' /etc/at.allow  
  
Access: (640/-rw-r-----) Owner: (root) Group: (daemon)  
-OR-  
Access: (640/-rw-r-----) Owner: (root) Group: (root)
```

Verify mode is `640` or more restrictive, owner is `root`, and group is `daemon` or `root`

Run the following command to verify `at.deny` doesn't exist, **-OR-** is:

- Mode `0640` or more restrictive
- Owned by the user `root`
- Group owned by the group `daemon` or group `root`

```
# [ -e "/etc/at.deny" ] && stat -Lc 'Access: (%a/%A) Owner: (%U) Group: (%G)'  
/etc/at.deny  
  
Access: (640/-rw-r-----) Owner: (root) Group: (daemon)  
-OR-  
Access: (640/-rw-r-----) Owner: (root) Group: (root)  
-OR-  
Nothing is returned
```

If a value is returned, verify mode is `640` or more restrictive, owner is `root`, and group is `daemon` or `root`

Remediation:

- **IF** - at is installed on the system:
Run the following script to:

- **/etc/at.allow:**
 - Create the file if it doesn't exist
 - Change owner or user **root**
 - If group **daemon** exists, change to group **daemon**, else change group to **root**
 - Change mode to **640** or more restrictive
- - **IF** - **/etc/at.deny** exists:
 - Change owner or user **root**
 - If group **daemon** exists, change to group **daemon**, else change group to **root**
 - Change mode to **640** or more restrictive







```
#!/usr/bin/env bash

{
  grep -Pq -- '^daemon\b' /etc/group && l_group="daemon" || l_group="root"
  [ ! -e "/etc/at.allow" ] && touch /etc/at.allow
  chown root:$l_group /etc/at.allow
  chmod u-x,g-wx,o-rwx /etc/at.allow
  [ -e "/etc/at.deny" ] && chown root:$l_group /etc/at.deny
  [ -e "/etc/at.deny" ] && chmod u-x,g-wx,o-rwx /etc/at.deny
}
```

References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

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.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002	M1018