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
T1040, T1040.000, T1056, T1056.001, T1557, T1557.000	TA0002	M1050

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 Disable Autorun and Autoplay for Removable Media Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	8.5 Configure Devices Not To Auto-run Content 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	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

2.1.3 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	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

2.1.4 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	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

2.1.5 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 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

2.1.6 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	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

2.1.7 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 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

2.1.8 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	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
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	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

2.1.11 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	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

2.1.12 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	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, 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 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
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 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
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	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

2.1.16 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	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

2.1.17 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	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

2.1.18 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 are 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	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

2.1.20 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 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	2.6 Address unapproved software 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.

Audit:

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 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
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 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