Security hardening task
Baseline configurations
Configuration checks
Disabling unused ports
Encryption using the latest standards
Firewall maintenance
Hardware & software disposal
Multifactor authentication (MFA)
Network access privileges
Network log analysis

Password policies
Patch updates
Penetration test (pen test)
Port filtering
Removing or disabling unused applications and services
Server and data storage backups

Description
A documented set of specifications within a system that is used as a basis for future builds, releases, and updates.
Updating the encryption standards for data that is stored in databases.
Ports can be blocked on firewalls, routers, servers, and more to prevent potentially dangerous network traffic from passing through.
Rules or methods used to conceal outgoing data and uncover or decrypt the incoming data.
Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats.
Ensures that all old hardware is properly wiped of all data and disposed of.
A security measure which requires a user to verify their identity in two or more ways to access a system or network. MFA options include a password, pin number, badge, one-time password (OTP) sent to a cell phone, fingerprint, and more.
Network access privileges involves permitting, limiting, and/or blocking access privileges to network assets for people, roles, groups, IP addresses, MAC addresses, etc.
The process of examining network logs to identify events of interest.

The National Institute of Standards and Technology's (NIST) latest recommendations for password policies focuses on using methods to salt and hash passwords, rather than requiring overly complex passwords or enforcing frequent changes to passwords.
A software and operating system (OS) update that addresses security vulnerabilities within a program or product.
A simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes.
A firewall function that blocks or allows certain port numbers to limit unwanted communication.
Unused applications and services can become a point of vulnerability because they are less likely to be maintained or updated with new security features.
Server and data storage backups help protect data assets from being lost. Backups can be recorded and stored in a physical location or uploaded/synced to a cloud repository.

Common uses
To restore a system to a previous baseline after a network outage, or unauthorized changes on a baseline.
To see if there are any unauthorized changes to the system.
Before an incident occurs, to prevent malicious actors from entering the network through the open port. Can be used after an incident to prevent future attacks from happening through unused open ports.
Can be implemented regularly to assess if the current encryption standards are secure and effective for your organization. The encryption standards can also be updated after a data breach.
This can happen regularly. Firewall rules can be updated in response to an event that allows abnormal network traffic into the network. This measure can be used to protect against various DDoS attacks.
Prevent the network from various threats by removing outdated or unused software or hardware that do not have the latest security patches or updates. Unpatched devices can allow malicious actors to easily access the network.
Can help protect against brute force attacks and similar security events. MFA can be implemented at any time, and is mostly a technique that is set up once then maintained.
Reduces the risk of unauthorized users and outside traffic from accessing the internal network. This can be implemented once, or revisited depending on the likelihood of social engineering or brute force attacks.
Can be configured to alert the security team when there is abnormal traffic on the network. This can be used either before an incident occurs, during to track network traffic, and can be configured in the response of a cybersecurity attack. A common tool used for analyzing network logs is a SIEM.

Password policies are used to prevent attackers from easily guessing user passwords, either manually or by using a script to attempt thousands of stolen passwords (commonly called a brute force attack).
Patch updates often contain fixes to security problems. It is important to keep systems up to date with the latest security patches because attackers will be alerted to the security vulnerability when patches are released. They will be more likely to target that vulnerability before people eventually apply the patches.
Pen tests are used to protect and prevent against potential attacks.
Port filtering is used to control network traffic and can prevent potential attackers from entering a private network.
This procedure is used to reduce potential vulnerabilities within a network.
Backups are used to restore lost data from attacks, human error, equipment failures, and other unplanned losses.

