ANALYSIS OF NETWORK HARDENING

Security hardening task	Description
Baseline configurations	A documented set of specifications within a system that is used as a basis for future builds, releases, and updates.
Configuration checks	Updating the encryption standards for data that is stored in databases.
Disabling unused ports	Ports can be blocked on firewalls, routers, servers, and more to prevent potentially dangerous network traffic from passing through.
Encryption using the latest standards	Rules or methods used to conceal outgoing data and uncover or decrypt the incoming data.
Firewall maintenance	Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats.
Hardware & software disposal	Ensures that all old hardware is properly wiped of all data and disposed of.
Multifactor authentication (MFA)	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	Network access privileges involves permitting, limiting, and/or blocking access privileges to network assets for people, roles, groups, IP addresses, MAC addresses, etc.
Network log analysis	The process of examining network logs to identify events of interest.
Password policies	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.
Patch updates	A software and operating system (OS) update that addresses security vulnerabilities within a program or product.
Penetration test (pen test)	A simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes.
Port filtering	A firewall function that blocks or allows certain port numbers to limit unwanted communication.
Removing or disabling unused applications and services	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	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.