**Hardening Concepts**

Network equipment, software, and operating systems use default settings from the developer or manufacturer which attempt to balance ease of use with security. Unfortunately these default configurations are an attractive target for attackers as they usually include well-documented credentials, allow simple passwords and use insecure protocols which increase the likelihood of successful cyberattacks. Therefore, it's crucial to change these default settings to improve security.

Hardening refers to the methods used to improve a device's security by changing its default configuration. There are various ways for hardening switches, routers, server hardware and operating systems.

**Switches & Routers**

* Change default credentials
* Disable unnecessary services and interfaces
* Use secure management protocols such as SSH and HTTPS instead of Telnet or HTTP
* Implement Access Control Lists
* Configure port security
* Enforce strong password policies

**Server Hardware and Operating Systems**

* Change default credentials
* Disable unnecessary services
* Apply security patches and updates
* Use firewalls and intrusion detection systems
* Secure configuration
* Enable logging and monitoring
* Use Antivirus and Antimalware solutions
* Enforce physical security