Mariam Mostafa Amin Mostafa
2205084

1. Systems Hardening: A process of securing a system through minimizing its vulnerable surface is what the hardening process entails. This is done by the removal of services not needed, turning off unused applications and ports, patching software vulnerabilities, enforcing proper access control, and other configurations to reduce risks. The idea is that hardening reduces as many avenues as possible through which vulnerabilities can be exploited and the system compromised.

Importance in Cybersecurity: Systems hardening is the core of any cybersecurity maintenance because it reduces the attack surface of a system, making it less vulnerable to attacks. It eliminates or secures unnecessary features; thus, only needed services are running, preventing unauthorized access, data breaches, and other cyberattacks. In addition, hardening minimizes risks from zero-day vulnerabilities, configuration errors, and weak passwords.

2. Types of Systems that Benefit from Hardening:
Servers: These are one of the primary devices that cybercriminals attack due to their crucial role in application, website, and data hosting. Hardening servers includes:
Disabling of unnecessary services or ports not utilized by the server.
Strong authentication such as multi-factor authentication.
Application of security patches and updates whenever available to avoid exploits.
Configurations of a firewall and IDS/IPS for monitoring suspicious activities.

Workstations: These are the points where employees connect into the network; therefore, they become one of the common entry points into systems, especially by cyber attackers. Hardening workstations includes:

Impacting strong password policies and enforcing password complexity.
Restricting administrative privileges and ensuring users only have access to the applications they need.
Installing endpoint protection software such as antivirus and anti-malware programs, which will help detect and prevent threats.
Enabling full disk encryption to protect data in case of theft.

Devices: Network Devices include Routers, Switches, and Firewalls. Network devices are at the core of any organization's IT infrastructure. As such, they should be

appropriately hardened to avoid unauthorized access and possible network breaches. This includes hardening like disabling unnecessary router/switch ports or services; strict access controls by restricting access to the management interfaces of the devices to trusted IP addresses; and adopting secure protocols for management instead of insecure ones, such as Telnet.

Regularly update the firmware to handle known vulnerabilities and apply security patches.

By hardening various systems, an organization will be able to make each separate system a different layer of defense that may reduce the overall possibility of successful cyber-attacks.