Mariam Mostafa Amin Mostafa
2205084

2. System Hardening Techniques
1. Disable Unnecessary Services
Explanation: One must turn off the services that are not needed by stopping or uninstalling software, processes, or functionality of the system that are not required for its basic functioning. For example, if there is no use of a server to provide web server or file-sharing services, these services must be turned off.

This contributes to system security because turning off unrequired services reduces the attack surface. Any particular service operating on a system might contain vulnerabilities that can otherwise be used by the attacker. In this way, it reduces the number of running services that become an entry point for the exploiters. In this way, it becomes very tough for any attacker to provide unauthorized access or privilege escalation.

2. Least Privilege Access
Explanations: The least privilege access describes the principle that grants any user, application, or process the minimal level of access they require to function correctly. For example, users who have the need to only read files should not have the capability to write and execute them. In a network context, users that need access to resources need only the resources or areas it requires, and by blocking access to the other areas, exposure is limited.

System Security Contribution: The system diminishes the threat of unauthorized access and, in the event of an occurrence, limits the effects of the breach. In cases where an attacker manages to compromise an account or a service, such an attack will be contained since that compromised entity does not have more privileges than required to alter or access other important parts of the system. This reduces the chances of lateral movement within the network.

3. Patch Management
Explanation: Patch management encompasses the regular deployment and management of patches, security updates, and fixes of known vulnerabilities. Vendors regularly release patches to overcome security vulnerabilities or bugs that might be used by an attacker.

Contribution to System Security: Patching and updating are very important to system security. Most cyber-attacks use known bugs in older versions of software. Regular patching ensures that systems stay updated with the most recent security fixes, reducing attackers' windows of vulnerability and substantially cutting the chance of becoming a victim. For zero-day exploits, patch management reduces the risk after patches become available to secure a system before the malicious usage of vulnerabilities can become feasible.

4. Configuration Baselines
Explanation: A configuration baseline is a pre-defined set of security configurations and settings that become the reference point for the secure setting up of systems. This might entail firewalls, account settings, network configurations, and other system settings known to be secure. Baselines act as a benchmark against which the security posture of a system is assessed to then find misconfigurations.

Contribution to System Security: Configuration baselines ensure that systems are set up consistently in a secure manner. This helps in sustaining system integrity and reducing human errors at system setup. In case there is any change in a system, it can be compared with the baseline for any deviation that might introduce a weakness or a vulnerability in its security. If any deviations are present, then the administrators can quickly identify and fix the security issues. Baselines also provide assistance during compliance audits, verifying if systems follow all standards and best practices in security.

5. Network Segmentation
Network Segmentation: This consists of segmenting a network into smaller, isolated segments, each with its own set of security controls. Segments could be carried out based on function-separating, for example, finance systems from HR systems-or department, such as developer systems from production systems-based on other criteria. Access between segments is controlled through firewalls, access control lists, or other network security devices.

Contribution towards System Security: Segmentation reduces the possibility of lateral movement on the network that an attacker might use. In such a case, an attacker is prevented from view or further access to other parts of a network since he remains isolated in a segment he has taken control over. This helps in containing security breaches and limiting the damage. For example, even in cases where an intruder is able to breach a segment of the network that is not so secure, it would be hard for him to easily migrate into areas of the network that concern the company's financial or

customer databases. Also, with segmentation, granular access control is possible, where security policies applicable for each segment may be enforced correspondingly.