Project Part 8: Windows Hardening Recommendations

Scenario

As a security administrator for Always Fresh, you have been instructed to ensure that Windows authentication, networking, and data access are hardened. This will help to provide a high level of security.

The following are issues to be addressed through hardening techniques:

- Previous attempts to protect user accounts have resulted in users writing long passwords down and placing them near their workstations. Users should not write down passwords or create passwords that attackers could easily guess, such as words founds in the dictionary.
- Every user, regardless of role, must have at least one unique user account. A user who operates in multiple roles may have multiple unique user accounts. Users should use the account for its intended role only.
- Anonymous users of the web server applications should only be able to access servers located in the demilitarized zone (DMZ). No anonymous web application users should be able to access any protected resources in the Always Fresh IT infrastructure.
- To protect servers from attack, each server should authenticate connections based on the source computer and user.

Tasks

Create a summary report to management that describes a hardening technique that addresses each issue listed above. Provide rationale for each selection.

Required Resources

- Internet access
- Course textbook

Submission Requirements

- Format: Microsoft Word (or compatible)
- Font: Arial, size 12, double-space
- Citation Style: Follow your school's preferred style guide
- Length: 2 to 4 pages

Self-Assessment Checklist

- I addressed all issues required for the summary report.
- I created a well-developed and formatted report with proper grammar, spelling, and punctuation.
- I followed the submission guidelines.