Project 3: Monitoring and Securing the DFI Environment

Connecting, Reporting, and Analysis

- Demonstrate an understanding of connecting and navigating inside of the provided computer environment.
- Demonstrate an understanding of the National Institute of Standards and Technology (NIST) Framework, Defense in Depth and document from Microsoft by performing an analysis of the security configuration on the servers provided.
- Demonstrate an understanding of the appropriate encryption for data in transit.
- Recommend at a very high level what should be automated and how.
- Understanding the needs of the organization (vis-à-vis the server configuration) with what is needed via NIST 800-43 and Microsoft's Security Update Guide the student will select the appropriate updates to install.

Firewalls and Intrusion Detection System (IDS) Configuration

- Demonstrate a basic understanding of firewall concepts and how to craft a simple firewall rule.
- Show a basic understanding of IDS concepts and how to craft a simple IDS rule.
- Prove a basic understanding of how to appropriately mitigate a threat via firewall alerts.

Encryption, Hashes, and Linux

- Demonstrate the ability to ensure executables are legitimate by comparing file hash with a known good copy or with a hash provided in advance.
- Demonstrate an understanding of how to log certain events, in this case, failed Remote Desk Protocol (RDP) attempts.
- Demonstrate an understanding of Linux permissions by creating directory and then assigning appropriate permissions.
- Produce a narrative status report that will tie all of the projects together in the form of a report to management.
- Demonstrate encrypting a directory.