Project: Monitoring and Securing the DFI Environment

Connecting, Reporting and Analysis

| **Success Criteria** | **Specifications** |
| --- | --- |
| The student will demonstrate an understanding of connecting and navigating inside the provided computing environment. | * Screenshot provided to show a proper connection to Windows Workstation using RDP * Screenshot provided to show a proper connection to the Linux server using SSH. |
| The student will demonstrate an understanding of the NIST Framework, Defense-in-Depth and documentation from Microsoft by performing an analysis of the security configuration on the servers provided. | * A report detailing 3 primary areas   + File Permissions that need modified   + Roles that are not needed on Windows server   + Any services that should or should not be running |
| The student will demonstrate an understanding of the appropriate encryption for data in transit. | * Choose one of the appropriate encryption methods from the documentation provided. Provide justification for the method you chose. |
| Automation is only discussed, not implemented. The students will be able to recommend at a very high level what should be automated and how. | * In report or table form, provide 3 areas where automation could be deployed to DFI. * Example: Area: Active Directory. The item for automation: Automatic account lockout if login from 2 geographically distant IPs. |
| Understanding the needs of the organization (vis-a-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 for install. | * The student will provide a table that lists at least 3 updates that should be installed and 3 updates that are not necessary. * Justify your recommendations as to why you are making your choices. |

Firewalls and IDS Configuration

| **Success Criteria** | **Specifications** |
| --- | --- |
| The students will demonstrate a basic understanding of firewall concepts and how to craft a simple firewall rule. | * Provide the commands necessary to complete the firewall rule given the scenario in the template. |
| The students will demonstrate a basic understanding of IDS concepts and how to craft simple IDS rules. | * Provide the commands necessary to complete both of the scenarios given in the template. * For documentation purposes, explain your commands for non-technical management. |
| Students will demonstrate a basic understanding of how to appropriately mitigate a threat via firewall alerts. | * The student will provide mitigation recommendations based on their analysis of the report with a focus on friend/foe of the source IP as well as an additional layer of protection for the destination IP. |

Encryption, Hashes and Linux

| **Success Criteria** | **Specifications** |
| --- | --- |
| Students will demonstrate the ability to ensure executables are legitimate by comparing file hash with a known good copy or with a hash provided in advance. | * Provide a screenshot that displays the command that was run as well as the file hash. |
| Students will demonstrate an understanding of how to log certain events, in this case, failed RDP attempts. | * Export the results to CSV on the server provided. * Open the CSV with notepad. * Provide a screenshot of the results |
| Students will demonstrate an understanding of Linux permissions by creating a directory and then assigning appropriate permissions. | * Create the directories listed in the request. * Create the groups listed in the request. * Create the users listed and place them in the appropriate groups. * Set the directory permissions where the groups are the owners of their respective directories. * Explain the syntax used for setting the permissions. |
| Students will produce a narrative 'status report' that will tie all of the projects together in the form of a report to management. | * Explain all of the tasks performed in the first two weeks. * Explain any recommendations for changes in permissions. * Tie all of the work done together in a big picture narrative. * Recommend the way forward for DFI in terms of security products (at least 2) and policies (also at least 2.) |
| Demonstrate encrypting a directory. | * Encrypt the deliverables in the previous steps using 7zip and a strong password. * Upload the file to Udacity for testing. * Provide the password to the file in the notes to the reviewer. |