Unit 2 Assignment

Outcomes addressed in this activity:

- Describe the use of network monitors including sniffers and system logs.
- Summarize infrastructure security, and operating system hardening and protection.
- Monitor and diagnose network security-related problems.
- Describe risk management best practices.

Course outcome:

IT286-1: Examine the process of risk assessment and network monitoring.

Instructions:

NOTE: You will have two parts to the Assignment in this unit that will be submitted as one file through the Dropbox.

Requirements:

Unit Assignments include short essay, descriptive tables, and screen captures demonstrating an understanding of the topics. Any resource used including the textbook should be properly cited.

Documents should be submitted using APA Style (double-spaced with a title page and a reference page). Essays should be separated into sections by the Assignment Part number and the question number.

Part 1

1. In a short essay, briefly explain the concept of hardening. Do some research on Windows Server™ hardening. Outline at least three ways to harden an operating system.

2. Create a table showing the three types of reporting systems outlined in the textbook.
   Method       Definition       Suggested Use

3. User account control is critical to network security. In a short essay, outline at least three best practices for managing user accounts.

4. Review the section in the textbook on detection controls and prevention controls. Create a table showing two of each. Include a description of each.

5. Identifying risks associated with monitoring ensures network administrators focus on those areas that are critical and identify gaps. Explain what you would include in a remediation policy for your company.

Part 2

Lab Questions and Screen Captures

Copyright Kaplan University
Assignment Grading Rubric

Course: IT286   Unit: 2   Points: 50

1. Review the video on `msconfig`. Open the program `msconfig` on your Windows system and select the Services tab. Select the heading Status. Click the heading to sort the services by Running and Stopped (alphabetical). Take a screen capture.

2. Open `msconfig` on your Windows system and select the Startup tab. Take a screen capture.

3. Open the Event Viewer on your Windows system and select Windows Logs, Security. Highlight a single event in the log and take a screen capture. With the event highlighted, look to the right under Actions and select Copy > Copy Details as Text. Copy to a Word document and include the first entries as part of your answer.

Example:
Log Name:    Security
Source:      Microsoft-Windows-Security-Auditing
Date:        7/30/2014 6:15:51 AM
Event ID:    4624
Task Category: Logon
Level:       Information
Keywords:    Audit Success
User:        N/A
Computer:    CM1050
Description: An account was successfully logged on.

Review the grading rubric below before beginning this activity:

Assignment grading rubric = 50 points

<table>
<thead>
<tr>
<th>Assignment Requirements</th>
<th>Points Possible</th>
<th>Points Earned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part 1: Essay Questions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. In a short essay, briefly explain the concept of hardening. Do some research on</td>
<td>0–10</td>
<td></td>
</tr>
<tr>
<td>Windows Server hardening. Outline at least three ways to harden an operating system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Create a table showing the three types of reporting systems. Method Definition</td>
<td>0–6</td>
<td></td>
</tr>
<tr>
<td>Suggested Use</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. User account control is critical to network security. In a short essay, outline at</td>
<td>0–6</td>
<td></td>
</tr>
<tr>
<td>least three best practices for managing user accounts.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4. Review the section in the textbook on detection controls and prevention controls. Create a table showing two of each. Include a description of each.还有很多的描述

5. Identifying risks associated with monitoring ensures network administrators focus on those areas that are critical and identify gaps. Explain what you would include in a remediation policy for your company.

### Part 2: Lab Questions and Screen Captures

1. Open `msconfig` on your Windows system and select the Services tab. Select the heading Status. Click the heading to sort the services by Running and Stopped (alphabetical). Take a screen capture.

2. Open `msconfig` on your Windows system and select the Startup tab. Take a screen capture.

3. Open the Event Viewer on your Windows system and select Windows Logs, Security. Highlight a single event in the log and take a screen capture. With the event highlighted, look to the right under Actions and select Copy > Copy Details as Text. Copy to a Word document and include the first entries as part of your answer.

---

<table>
<thead>
<tr>
<th>Total (Sum of all points)</th>
<th>0–50</th>
</tr>
</thead>
</table>

Less deduction taken for spelling, grammar, and APA errors. Plagiarism is totally unacceptable.

New total after deductions