Unit 4 Assignment

Outcomes addressed in this activity:

- Describe authentication and access control.
- Examine single factor and multifactor authentication methods.
- Discuss the use of access control methods such as smart cards, Common Access Cards (CAC), and access control lists (ACLs).
- Describe the use of authentication and tunneling protocols.

Course outcome:

IT286-2: Investigate device and infrastructure security, access control, authentication, and authorization.

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. Authentication is based on one or more of five factors. Create a table of these five.
   Factor | Example

2. In a short essay describe the pros and cons of implementing a single factor authentication system and of implementing a multifactor authentication system. Cite your resources.

3. In a short essay explain Layered Security and Defense in Depth. Give an analogy for the philosophy behind this from another area (Example: physical access to a military base).

4. In a short essay describe Transitive Access. Explain why this is an important technique for large networks.

5. There are four primary methods of access control (Example: Mandatory Access Control). Create a table of these four and describe them.
   Access Control Method | Definition

6. Create a table that summarizes the five tunneling protocols outlined in the text.
   Protocol | Definition | Use
Part 2

Lab Questions and Screen Captures

1. Set up Auditing of Logins
Microsoft Windows operating systems (Windows 7™, Windows 8™ and Windows Server) can be configured to audit various events and to create logs of those events. Follow the instructions below to enable a login auditing.
   a. Open the Control Panel. In Control Panel, (System and Security) double-click Administrative Tools, and then click Local Security Policy.
   b. In Local Security Settings, double-click Local Policies, double-click Audit Policy, and then highlight the event that you want to audit and right click. (Example: Audit logon events - Success, Failure and Audit logon events - Success, Failure.)
   c. To view the event logs, click Start, point to Programs, point to Administrative Tools, and then click Event Viewer. Check the log for the event.
   d. Did you see your login event? Take a screen capture of your login event.

2. Examine firewall configurations for access control
Review the Windows Firewall dialog box below. Notice the selection Don't allow exceptions check box.
By selecting this check box Windows Firewall blocks all unsolicited requests to connect to the computer. Notice the Exceptions tab. When the Don’t allow exceptions box is checked even entries listed in exceptions will be denied.

If Windows Firewall is active on your computer and you want additional protection in a public area such as a coffee shop, select the Don’t allow exceptions setting.

If you select the Exceptions tab, you can also set a configuration to allow a port access through the firewall. Use the Edit a Port dialog box to configure the Name and Port number.

What firewall is active on your system? Examine the settings. Take a screen capture.

3. Identify User Accounts with Administrator Access
   This lab requires a Windows 7 or Windows 8 operation system.
   User management is simplified by adding users to groups. To see which users are members of the Administrators group, follow these steps:
   a. Choose Start, Control Panel, Administrative Tools
   b. Choose Computer Management and open it.
   c. Within the left pane, expand Local Users And Groups and then expand Groups.
   Take a screen capture.
d. Double-click **Administrators**. The Administrators Properties box appears showing a list of members *(Do not remove a user without verifying there is another user with administrative rights.)*. Exit the Computer Management console.

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><strong>Part 1: Essay Questions</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Authentication is based on one or more of five factors. Create a table of these five.</td>
<td>0–5</td>
<td></td>
</tr>
<tr>
<td>Factor</td>
<td>Example</td>
<td></td>
</tr>
<tr>
<td>2. In a short essay describe the pros and cons of implementing a single factor authentication system and of implementing a multifactor authentication system. Cite your resources.</td>
<td>0–6</td>
<td></td>
</tr>
<tr>
<td>3. In a short essay explain Layered Security and Defense in Depth. Give an analogy for the philosophy behind this from another area (Example: physical access to a military base).</td>
<td>0–8</td>
<td></td>
</tr>
<tr>
<td>4. In a short essay describe Transitive Access. Explain why this is an important technique for large networks.</td>
<td>0–5</td>
<td></td>
</tr>
<tr>
<td>5. There are four primary methods of access control (Example: Mandatory Access Control). Create a table of these four and describe them.</td>
<td>0–6</td>
<td></td>
</tr>
<tr>
<td>Access Control Method</td>
<td>Definition</td>
<td></td>
</tr>
<tr>
<td>6. Create a table that summarizes the five tunneling protocols outlined in the text.</td>
<td>0–10</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>Definition</td>
<td>Use</td>
</tr>
<tr>
<td><strong>Part 2: Lab Questions and Screen Captures</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Set up Auditing of Logins. Take a screen capture. Did you see your login event? Take a</td>
<td>0–3</td>
<td></td>
</tr>
<tr>
<td>Screen capture of your login event.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td><strong>2. Examine Windows Firewall configurations for access control.</strong> What firewall is active on your system? Examine the settings. Take a screen capture.</td>
<td>0–3</td>
<td></td>
</tr>
<tr>
<td><strong>3. Identify User Accounts with Administrator Access.</strong> Take a screen capture.</td>
<td>0–4</td>
<td></td>
</tr>
<tr>
<td><strong>Total (Sum of all points)</strong></td>
<td>0–50</td>
<td></td>
</tr>
</tbody>
</table>

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

New total after deductions