Unit 5 Assignment

Outcomes addressed in this activity:

- Discuss wireless technology including wireless protocols, wireless devices, and wireless security.
- Explain various types of wireless attacks and methods to mitigate these attacks.
- Examine appropriate control mechanisms to secure data in virtualized environments and on the cloud.

Course outcome:

IT286-3: Explain the protection of wireless networks and cloud services, and the hardening of hosts and applications.

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. Create a table comparing WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) and WPA2

<table>
<thead>
<tr>
<th>Standard</th>
<th>Definition</th>
<th>Algorithm</th>
<th>Suggested Use</th>
</tr>
</thead>
</table>

2. In a short essay, describe Temporal Key Integrity Protocol (TKIP). What is it based on? What does it do?

3. You are asked to secure a wireless network by making sure only authorized computers connect. What can you do to accomplish this? Give an example.

4. Review Table 5.1 in your text that lists six different types of wireless attacks and matches an analogy of each attack. Do some research on these attacks and create a table of your findings.

<table>
<thead>
<tr>
<th>Attack Name</th>
<th>Definition</th>
<th>Result</th>
</tr>
</thead>
</table>

5. In a short essay, define the three cloud computing service models.

6. In a short essay, examine the cloud computing delivery models. Give a scenario for each.

7. The following five topics describe important concepts for virtualizations: Snapshots, Patch Compatibility, Host Availability/Elasticity, Security Control Testing (SCT) and Sandboxing. Briefly define each of these and explain why it can be a security concern.
Part 2

Lab Questions and Screen Captures

1. Connect a wireless network on a Windows system
View the video on wireless connections before doing this lab.

To set up a new wireless connection, select **Set up a new network** from the Network and Sharing Center window.

![Set Up a Connection or Network](image)

Choose a connection option

- **Connect to the Internet**
- **Set up a wireless, broadband, or dial-up connection to the Internet**

To enable an automatic wireless network configuration, select the wizard.

![Manually connect to a wireless network](image)

How do you want to add a network?

- **Manually create a network profile**
  
  This creates a new network profile or locates an existing network and saves a profile for the network on your computer. You need to know the network name (SSID) and security key (if applicable).

To manually connect to a wireless network, select the **Manually create a network profile**. To connect to an existing wireless network under **Available networks**, select the network name and then **Configure**. In **Wireless Network Properties**, specify the wireless network settings and specify the network name SSID (Service Set Identifier). *Using only the SSID is not secure.* Take a screen capture of the settings.

2. Wireless Capture Tools
*Note: Be cautious when downloading any software tool from insecure websites.*

Review a wireless packet sniffer tool (see suggestions below) and provide a brief description. Take a screen capture of the output data from the tool as shown on the wireless packet sniffer website (if not available, show features).

**Suggestions:**
- Aircrack-ng - a set of tools for auditing wireless networks
- NetStumbler – wardriving to find open wireless access points
- InSSIDer – signal strength and access point finder, etc.

3. Platform as a Service

Review a Platform as a Service (PaaS) vendor (Ex: Salesforce.com or Amazon Web Services) and describe how the client interacts with the cloud using this service. Outline several of the features of the platform and take a screen capture of the vendor’s marketing site and graphics.

Review the grading rubric below before beginning this activity:
### Assignment Grading Rubric

**Course:** IT286  **Unit:** 5  **Points:** 50

---

**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. Create a table comparing WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) and WPA2. Standard Definition Algorithm Suggested Use</td>
<td>0–5</td>
<td></td>
</tr>
<tr>
<td>2. In a short essay, describe Temporal Key Integrity Protocol (TKIP). What is it based on? What does it do?</td>
<td>0–4</td>
<td></td>
</tr>
<tr>
<td>3. You are asked to secure a wireless network by making sure only authorized computers connect. What can you do to accomplish this? Give an example.</td>
<td>0–4</td>
<td></td>
</tr>
<tr>
<td>4. Review Table 5.1 in your text that lists six different types of wireless attacks and matches an analogy of each attack. Do some research on these attacks and create a table of your findings. Attack Name Definition Result</td>
<td>0–6</td>
<td></td>
</tr>
<tr>
<td>5. In a short essay, define the three cloud computing service models.</td>
<td>0–3</td>
<td></td>
</tr>
<tr>
<td>6. In a short essay, examine the cloud computing delivery models. Give a scenario for each.</td>
<td>0–8</td>
<td></td>
</tr>
<tr>
<td>7. The following five topics describe important concepts for virtualizations: Snapshots, Patch Compatibility, Host Availability/Elasticity, Security Control Testing (SCT) and Sandboxing. Briefly define each of these and explain why it can be a security concern.</td>
<td>0–10</td>
<td></td>
</tr>
<tr>
<td><strong>Part 2: Lab Questions and Screen Captures</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Connect a wireless network on a Windows system. Take a screen capture.</td>
<td>0–3</td>
<td></td>
</tr>
</tbody>
</table>

---

Copyright Kaplan University
<table>
<thead>
<tr>
<th>Task</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Review a wireless packet sniffer tool. Take a screen capture.</td>
<td>0–3</td>
</tr>
<tr>
<td>3. Review a Platform as a Service (PaaS) vendor. Take a screen capture.</td>
<td>0–4</td>
</tr>
<tr>
<td><strong>Total (Sum of all points)</strong></td>
<td>0–50</td>
</tr>
</tbody>
</table>

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

**New total after deductions**