Portfolio Activity: Analyze a vulnerable system for a small business

Activity Overview

In this activity, you will conduct a vulnerability assessment for a small business. You will evaluate the risks of a vulnerable information system and outline a remediation plan

A vulnerability assessment is the internal review process of an organization's security systems. As a cybersecurity analyst, you might help with vulnerability assessments to prevent attacks in an organization. Later, you can add this document to your cybersecurity portfolio, which you can share with prospective employers or recruiters. To review the importance of building a professional portfolio and options for creating your portfolio, read Create a cybersecurity portfolio.

Be sure to complete this activity and answer the questions that follow before moving on. The next course item will provide you with a completed exemplar to compare to your own work.

Scenario

Review the following scenario. Then complete the step-by-step instructions.

You are a newly hired cybersecurity analyst for an e-commerce company. The company stores information on a remote database server, since many of the employees work remotely from locations all around the world. Employees of the company regularly query, or request, data from the server to find potential customers. The database has been open to the public since the company's launch three years ago. As a cybersecurity professional, you recognize that keeping the database server open to the public is a serious vulnerability.

A vulnerability assessment of the situation can help you communicate the potential risks with decision makers at the company. You must create a written report that clearly explains how the vulnerable server is a risk to business operations and how it can be secured.

Step-By-Step Instructions

Follow the instructions to complete each step of the activity. Then, answer the 5 questions at the end of the activity before going to the next course item to compare your work to a completed exemplar.

Part 1 - Open a report template

Step 1: Access the template

Using a pre-formatted template can be a helpful starting point when constructing a written report. By providing pre-made layouts and headings, templates can provide a professional appearance.

To use the template for this course item, click the following link and select *Use Template*.

Link to template: Vulnerability assessment report

OR

If you don't have a Google account, you can download the template directly from the following attachment.

Vulnerability assessment report

DOCX File

Step 2: Access supporting materials

The following supporting materials will help you complete this activity. Keep them open as you proceed to the next steps. You will use this resource in Part 2 of this activity.

To use the supporting materials for this course item, click the link and select *Use Template*.

Link to supporting materials: NIST SP 800-30 Rev. 1

OR

If you don't have a Google account, you can download the supporting materials directly from the following attachment.

NIST SP 800-30 Rev. 1

DOCX File

Step 3: Review information about the vulnerable server

Vulnerability assessments typically include a description of the system being evaluated and the scope of the project.

Review the System Description and Scope of the *Vulnerability assessment report*.

The System Description highlights the relevant components, architecture, and dependencies of the system being assessed. All of these parts and connections make up the attack surface of the vulnerable information system.

The Scope specifies the focus and boundaries of the assessment. For example, you might specify that the scope of this assessment only relates to the confidentiality, availability, and integrity of the data on the server—not the physical security of the server or its related IT systems.

Part 2 - Perform a risk assessment

Step 1: Explain the purpose of the information system

You'll need to use the NIST SP 800-30 Rev. 1 resource to complete the risk assessment portion of the activity.

In addition to a system description and scope, vulnerability assessments commonly Include a purpose statement. This section helps stakeholders understand the underlying objective and intended outcome of your analysis. A purpose statement also connects the technical objectives of your analysis with the organization's goals.

Consider what you know about the server:

- *How is the database server valuable to the business?*
- *Why is it important for the business to secure the data on the server?*
- *How might the server impact the business if it were disabled?*

In the Purpose section of the report, use the preceding questions to help you write 3-5 sentences (60-100 words) describing the reason(s) for conducting this vulnerability analysis.

Step 2: Identify potential threat sources

Explore the *Threat sources* section of the *NIST SP 800-30 Rev. 1* resource. Using what you know about the vulnerable database server, notice the threat types and examples described.

In the Threat Source column of the Risk Assessment table of your template, identify three potential threats. Choose the threats using your best judgment and understanding of the earlier sections of the report.

Step 3: Identify potential threat events

NIST SP 800-30 Rev. 1 provides a comprehensive list of possible security incidents that could compromise a vulnerable information system—labeled *Threat events*. The list considers the average intent and capabilities of the threat source categories of the publication.
For example, a business competitor might have the technical capabilities needed to conduct a denial of service attack.
Explore the *Threat events* section in the resource. Then, identify three *reasonable* threat events that could be initiated, based on the threat sources you identified. Write the three threat events in the Threat Event column of the Risk Assessment table in your template.

Step 4: Calculate the risk of potential threats

You may recall from an earlier reading about calculating risks that potential threats and vulnerabilities are important factors to think about when evaluating the security of an asset.
Refer to the likelihood and severity sections of the *NIST SP 800-30 Rev. 1* resource and ask yourself the following questions about each threat that you identified earlier:

- *How frequently could this happen?*
- *Would critical business functions be impacted?*
- *How might this affect the business and its customers?*

Then, estimate a Likelihood score (1-3) and Severity score (1-3) for each threat and add your scores to the corresponding columns of the Risk Assessment table in your template. After, calculate an overall Risk score (1-9) for each threat using the formula (likelihood x severity = risk).
Note: The number of rows in a risk table can vary depending on the complexity and scope of the assessment. In general, it should provide stakeholders with a comprehensive overview of all significant risks.

Part 3 - Propose security recommendations

Step 1: Explain your approach

Another section that's commonly included in a vulnerability assessment is an explanation of your approach. This helps stakeholders understand your thought process of evaluating the risks you've identified—adding valuable context for stakeholders.
In the Approach section of your template, write 3-5 sentences (60-100 words) explaining why you selected the 3 specific threat sources/events you chose and why you think they're significant business risks.

Step 2: Propose a remediation strategy

Overall, a vulnerability assessment report should outline a strategy for addressing the risks of the target system. When possible, it should provide stakeholders with actionable steps that can be taken to remediate, or fix, vulnerabilities to avoid threats.
Note: Certain threats cannot be fixed. In those cases, it's equally important to consider a *mitigation strategy*—a plan to reduce the severity of a threat.
Think about security controls that could mitigate and/or remediate the risks you've identified:

- Principle of least privilege
- Defense in depth
- Multi-factor authentication (MFA)
- Authentication, Authorization, Accounting (AAA) framework

In the Remediation section of the template, write 3-5 sentences (60-100 words) summarizing specific security controls that can remediate or mitigate the risks to the information system.

Align your suggestions with the risks you've assessed. For example, suggesting public key infrastructure (PKI) to address exfiltration of sensitive information.

Pro Tip: Save the template

Finally, be sure to save a copy of your completed activity. You can use it for your professional portfolio to demonstrate your knowledge and/or experience to potential employers.

What to Include in Your Response

Be sure to address the following elements in your completed activity:

- 3-5 sentences describing the reasons for conducting the security analysis in the Purpose section
- A completed Risk Assessment section
- 3-5 sentences explaining your reasoning for the identified risks in the Approach section
  3-5 sentences summarizing a *remediation* and/or *mitigation* strategy in the Remediation section

Step 3: Assess your activity

The following is a self-assessment for your *Vulnerability assessment report*. You will use these statements to review your own work. The self-assessment process is an important part of the learning experience because it allows you to *objectively* assess your report.

There are a total of 5 points possible for this activity and each statement is worth 1 point. The items correspond to each step you completed for the activity.

To complete the self-assessment, first open your *Vulnerability assessment report*. Then, respond yes or no to each statement.

When you complete and submit your responses, you will receive a percentage score. This score will help you confirm whether you completed the required steps of the activity. The recommended passing grade for this activity is at least 80% (or 4/5 points). If you want to increase your score, you can revise your project and then resubmit your responses to reflect any changes you made. Try to achieve at least 4 points before continuing on to the next course item.