Congratulations! You passed!

Grade received 100% **Latest Submission Grade** 100% **To pass** 80% or higher

Go to next item

To pass this course item, you must complete the activity and receive at least 80%, or 4 out of 5 points, on the questions that follow. Once you have completed the activity and questions, review the feedback provided. You can learn more about graded and practice items in the course overview.

Activity Overview

In this activity, you will finalize the incident handler's journal that you've been working on throughout this course. Then, you'll add this document to your cybersecurity portfolio, which you can share with prospective employers or recruiters.

You may recall that in a previous activity at the introduction of this course, you completed your first entry in your incident handler's journal. As you progressed through this course, you used your incident handler's journal to apply your documentation skills and keep track of your learning journey. By now, you might have multiple entries in your journal. These entries would be valuable to add to your portfolio. To review the importance of building a professional portfolio and options for creating your portfolio, read Create your 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.

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 - Access your incident handler's journal

To complete this activity, you'll need to access your incident handler's journal. If you have saved your incident handler's journal, open it now and keep it open throughout this activity.

Step 1: Access the template

If you haven't saved or begun using your incident handler's journal, click the following link and select *Use Template.*

Link to template: Incident handler's journal

OR

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

Incident handler's journal
DOCX File

Step 2: Review your journal entries

You might have multiple entries in your incident handler's journal. If your journal contains missing or incomplete entries, go back and review any previous sections of this course to add additional log entries to your journal. Here's a list of the course activities you can revisit to complete your journal:

- Activity: Document an incident with an incident handler's journa
- Activity: Analyze your first packet
- Activity: Capture your first packet
- Activity: Investigate a suspicious file hash
- Activity: Use a playbook to respond to an attack
- Activity: Review a final report
- Activity: Explore signatures and logs with Suricata
- Activity: Perform a query with Splunk
- Activity: Perform a query with Chronicle

At minimum, you should have the following entries in your incident handler's journal:

- *At least* 4 dated and numbered journal entries, including:
  - 2 journal entries documenting an incident investigation using the 5 W's
  - 2 journal entries describing the use of a cybersecurity tool

Review your incident handler's journal and make any necessary changes. Here are some things to consider during your review:

- Errors in grammar, punctuation, and spelling
- Missing, inaccurate, or incomplete journal entries

Step 3: Update your journal entries

Update the journal entries that record an incident investigation.

In the **Description** section in a journal entry in your incident handler's journal, include a brief description of the entry (20-50 words). You can also identify which phase(s) of the NIST Incident Response Lifecycle the incident investigation occurred in and why. As a refresher, the phases are: *Preparation; Detection and Analysis; Containment, Eradication, and Recovery; and Post-Incident Activity.*

Part 2 - Complete your incident handler's journal

Step 1: Write a reflection entry

Take a moment to reflect on your learning journey in this course so far. Copy and paste the following questions into the **Reflections/Notes** section in your incident handler's journal. Then, write a two to three sentence response (40-60 words) to each question.

1. Were there any specific activities that were challenging for you? Why or why not?
2. Has your understanding of incident detection and response changed since taking this course?
3. Was there a specific tool or concept that you enjoyed the most? Why?

Pro Tip: Save a copy of your work

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 in your completed activity:

- 4 completed journal entries, with the **Date**, **Entry**, and **Description** section filled in (50-80 words)
- 2 of the 4 entries document an incident investigation in the **The 5 W's** section (4-6 sentences or bullet points)
- 2 of the 4 entries outline the use of a cybersecurity tool in the **Tool(s) used** section (3-5 sentences or bullet points)
-
- The **Reflections/Notes** section addresses the reflection prompt (6-9 sentences or bullets)

Note: *Some of these items may be addressed in the same journal entry. For example, a journal entry might contain descriptions about a cybersecurity tool and the 5 W's of an incident.*

Step 2: Assess your activity

The following is a self-assessment for your incident handler's journal. 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 incident handler's journal.

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 incident handler's journal. 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 project 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.

1. Your incident handler's journal contains at least four dated and numbered journal entries. **1 / 1 point**

- (•) Yes
- ( ) No

Correct

2. In the **Description** section of your incident handler's journal, you have included a brief description of the journal entry. **1 / 1 point**

- (•) Yes
- ( ) No

Correct

3. In **The 5 W's** section of your incident handler's journal, you have included at least two journal entries that record the details of an incident investigation using the 5 W's of an incident. **1 / 1 point**

- (•) Yes
- ( ) No

Correct

4. In the **Tool(s) used** section of your incident handler's journal, you have included at least two journal entries describing the use and purpose of a cybersecurity tool. **1 / 1 point**

- (•) Yes
- ( ) No

Correct

5. In the **Reflection/Notes** section of your incident handler's journal, you have included an entry that answers the reflection questions. **1 / 1 point**

- (•) Yes
- ( ) No

Correct