Activity Exemplar: Apply OS hardening techniques

Here is a completed exemplar along with an explanation of how the exemplar fulfills the expectations for the activity.

Completed Exemplar

To review the exemplar for this course item, click the link below and select *Use Template*.

- Security incident report exemplar
- The exemplar explained: Security incident report

OR

If you don't have a Google account, you can download the exemplar and incident report directly from the attachment below.

Security incident report exemplar
DOCX File

The Exemplar Explained - Security incident report exemplar
DOCX File

Assessment of Exemplar

Compare the exemplar to your completed activity. Review your work using each of the criteria in the exemplar. What did you do well? Where can you improve? Use your answers to these questions to guide you as you continue to progress through the course.

Note: *The exemplar represents one possible explanation for the issues that the end users are facing. Yours will likely differ in certain ways. What's important is that you identified the network protocols involved and created a report. In your role as a security analyst, you and your team would document any issue that occurs on the network and come up with solutions to help prevent the same issues from occurring in the future. Good quality documentation can save you and your organization time and potentially manage the attack early on.*

First, analyze the DNS & HTTP traffic log to identify a network protocol. Then, document the cybersecurity incident. Finally, recommend one security measure your organization could implement to prevent brute force attacks in the future. Creating this process will, in turn, help improve the organization's security posture.

The exemplar is accompanied by the activity, and presents a professional documentation example to include the following:

- One network protocol identified during the investigation
- Documentation of the incident
- A recommended security measure

Key Takeaways

As a security analyst, you might not always know exactly what is the primary cause of a network issue or a possible attack. But being able to analyze the protocols involved will help you make an informed assumption about what happened. This will allow you and your team to begin resolving the issue.