☰ Item Navigation

Activity Exemplar: Analyze network attacks

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 following link and select *Use Template.*

Cybersecurity incident report exemplar

OR

If you don’t have a Google account, you can download the exemplar directly from the attachment.

Cybersecurity 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 user is 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 make a best guess about what happened and then investigate further to troubleshoot the issue and strengthen the overall security of your network.*

The exemplar identifies that the connection timeout message is a result of a DoS attack. In this instance, the specific DoS attack is a SYN flood attack.

To determine this, analyze the data presented in the log file excerpt attached to this activity. Next, reflect on your current understanding of network attacks to identify what type of attack is occurring based on the data available.

After identifying a possible network attack type, proceed to explain how we came to identify the attack. Then, document how this specific type of attack might have affected the network and include a general description of how the attacker exploited the network vulnerability.

Lastly, describe how this attack resulted in the webpage displaying the connection timeout error.

The exemplar only provides one example of an explanation for the event. Describing an event typically requires presenting your evidence and explaining how you came to your decision. All patterns you notice in the logs and data are critical in determining the source and the type of network attack. The more practice you have identifying these patterns, the easier it will be to spot network attacks as they are occurring. This will allow you to respond to incidents more quickly and efficiently.

Mark as completed

Like Dislike Report an issue