Activity Exemplar: Analyze network layer communication

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 links and select *Use Template*.

Cybersecurity incident report exemplar

Cybersecurity incident report exemplar explained

OR

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

Cybersecurity incident report exemplar network traffic analysis
DOCX File

The Exemplar Explained - Cybersecurity Incident Report_ Network Traffic Analysis
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 offers one possible approach to investigating and analyzing a possible security event. 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.*

Writing an effective cybersecurity analysis report can help troubleshoot network issues and vulnerabilities more quickly and effectively. The more practice you have analyzing network traffic for suspicious trends and activity, the more effective you and your team will be at managing and responding to risks that are present on your network.

Key takeaways

As a security analyst, you may not always know exactly what is at the root of a network issue or a possible attack. But being able to analyze the IP packets involved will help you make a best guess about what happened or potentially prevent an attack from invading the network. The network protocol and traffic logs will become the starting point for investigating the issue further and addressing the attack.

Mark as completed