Step-By-Step Instructions

Follow the instructions and fill in the sections to complete the activity.

Step 1: Access the template

Access the template (Cybersecurity incident report network traffic analysis)

Step 2: Access supporting materials

The following supporting materials will help you complete this activity.

Access the template (Cybersecurity incident report network traffic analysis explanation)

Step 3: Provide a summary of the problem found in the DNS and ICMP traffic log

The network traffic analyzer tool inspects all IP packets traveling through the network interfaces of the machine it runs on. Network packets are recorded into a file. After analyzing the data presented to you from the DNS and ICMP traffic log, identify trends in the data. Assess which protocol is producing the error message when resolving the URL with the DNS server for the yummyrecipesforme.com website. Recall that one of the ports that is displayed repeatedly is port 53, commonly used for DNS. In your analysis:

- Include a brief summary of the DNS and ICMP log analysis and identify which protocol was used for the ICMP traffic.
- Provide a few details about what was indicated in the logs.
- Interpret the issues found in the logs.

Record your responses in part one of the cybersecurity incident reports.

Step 4: Explain your analysis of the data and provide one solution to implement

Now that you've inspected the traffic log and identified trends in the traffic, describe why the error messages appeared on the log. Use your answer in the previous step and the scenario to identify the reason behind the ICMP error messages. The error messages indicate that there is an issue with a specific port. What do the different protocols involved in the log reveal about the incident? In your response:

- State when the problem was first reported.
- Provide the scenario, events, and symptoms identified when the event was first reported.
- Describe the information discovered while investigating the issue up to this point.
- Explain the current status of the issue.
- Provide the suspected root cause of the problem.

Record your responses in part two of the cybersecurity incident report.

What to Include in Your Response

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

- Provide a summary of the problem found in the DNS and ICMP traffic log
- Explain your analysis of the data and provide one possible cause of the incident