Step-By-Step Instructions

Step 1: Access the template

Get the **Template** to complete the assessment.

Step 2: Access supporting materials

Use the supporting materials **"How to read a Wireshark TCP/HTTP log"** to understand log.

Step 3: Identify the type of attack causing this network interruption

As a security analyst, identifying the type of network attack based on the incident is the first step to managing the attack and preventing similar attacks in the future.

Here are some questions to consider when determining what type of attack occurred:

- What do you currently understand about network attacks?
- Which type of attack would likely result in the symptoms described in the scenario?
- What is the difference between a denial of service (DoS) and distributed denial of service (DDoS)?
- Why is the website taking a long time to load and reporting a connection timeout error?

Review the Wireshark reading from step 2 and try to identify patterns in the logged network traffic. Analyze the patterns to determine which type of network attack occurred. Write your analysis in section one of the Cybersecurity incident report template provided.

Step 4: Explain how the attack is causing the website to malfunction

Review the Wireshark reading from step 2, then write your analysis in section two of the Cybersecurity incident report template provided.

When writing your report, discuss the network devices and activities that are involved in the interruption. Include the following information in your explanation:

- Describe the attack. What are the main symptoms or characteristics of this specific type of attack?
- Explain how it affected the organization's network. How does this specific network attack affect the website and how it functions?
- Describe the potential consequences of this attack and how it negatively affects the organization.
- *Optional:* Suggest potential ways to secure the network so this attack can be prevented in the future.

What to Include in Your Response

Be sure to address the following in your completed activity:

- The name of the network intrusion attack
- A description of how the attack negatively impacts network performance