THWARTING CYBER ADVERSARIES

Scenario 1

External Attack Against A Webserver

General Information

In this scenario an external bad actor launched a series of attacks against a webserver (**IP address – 45.33.72.47)** in the cyber defense lab environment. Using alerts generated by the security information and events management system (SIEM), detect, and analyze this suspicious activity. The figure below shows the steps you should follow in solving this challenge. Each step has one or more associated questions that should be answered.

Event Timeline	Scenario Complexity	Estimated Completion Time
June 8, 2020 (00:00 to 23:30)	Simple	30 to 45 minutes

	Target Competencies	CWF Ref
1.	Working knowledge of characterizing and analyzing network traffic to identify anomalous activity and potential threats to network resources.	T0023
2.	Ability to correlate security events using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack	T0166
3.	Ability to analyze network alerts received from various sources within the enterprise to determine possible courses of such alerts	T0214