|  |  |
| --- | --- |
| **Course Code & Number: Name:** | |
| **Course Developer/Author:  Email:** | **eLearning Instructional Designer: Nickolas Gallegos** |

**Module Number and Title:** Directly from the *Course Design Plan: Modules* section. You will create a module design plan for each module on that document.

|  |
| --- |
| **Log Analysis Activity** |

Module Overview: Directly from the *Module Overview* column from the *Course Design Plan: Modules* section*.*

|  |
| --- |
| **In this module, students will learn about log files and how they are used during and after a cyber event has occurred.** |

Module Objectives:In the space below, provide the module objectives. There are typically 1 – 5 module objectives that describe what the students will be able to do after completing this module.Identify the course objective(s) that align with each module objective and, if necessary, describe the relationship. Objectives should encourage higher level thinking. *For assistance with writing effective course objectives, please refer to these resources:* [Bloom’s Taxonomy](http://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/) *and* [OPA Resource](http://www.depts.ttu.edu/opa/resources/docs/Program_Assessment_Handbook_4_13_2015.pdf) (page 7)*.*

**For K-12 courses,** **leave the Module Objectives blank in the beginning**—you will align modules to TEKS first, and then, at the end of development, you will write succinct module objectives that integrate TEKS with the actual tasks of the module.

| **Module Objectives**  By the completion of this module, students will be able to: | **Bloom’s Taxonomy Level** | **Assessment Strategy** | **Course Objectives Alignment (#)** |
| --- | --- | --- | --- |
| 1. Identify when a potential cyber event has occurred from a log file | Understand |  |  |
| 1. Perform basic analysis techniques to interpret information from a log file | Apply |  |  |
| 1. Find log files in their own computer systems and experimentally perform some log analysis techniques | Analyze |  |  |

Task Outline:In the table below, provide a title for each task students will need to complete in order to learn the topic/content. Describe the task and the reasoning for including in this module. Finally, note the module objective(s) that each task aligns with. **For K-12 courses,** list the detailed TEKS item that the task aligns with or supports (TEKS 1A, 1B, etc.). A K-12 example has been provided to illustrate how this document works. [Gagne’s Nine Events of Instruction](http://citt.ufl.edu/tools/gagnes-9-events-of-instruction/)

|  |  |  |  |
| --- | --- | --- | --- |
| **Step # of** [Gagne’s Nine Events…](http://citt.ufl.edu/tools/gagnes-9-events-of-instruction/) | **Task Title** | **Task Description/Rationale**   1. Write in first or second person, addressing students directly. 2. Include rationale or purpose for the task. Relate to Module Objectives where appropriate. 3. Explicit instructions for completing the task. | **Module Objective Alignment (#) or TEKS** |
| *1* | *Opening Activity* | *Below is a new clip about a controversial issue in the last presidential election. As you learn more about the presidency in this lesson, you’ll be able to look back on what you see here and decide if your understanding of this event has changed at all. Watch the video, take a few notes, and then take the Lesson Opener quiz to make sure you understood the most important parts.[link to video]* | 8B, 10B, 11C |
| 1 | Discuss log files | We will discuss what a log file is and how it’s used to help ensure a system or application is running correctly or for use in forensics after a cyber event has occurred. |  |
| 2 | Look at some log files and understand how they are formatted | Open a log file in the system being used. Analyze the basic information within the logs and understand what it means. |  |
| 3 | Analyze a log file that contains a cyber event | Look at a log file with the students and walk through the analysis process. Have them follow along on their own machine and execute collection, parsing, and grouping/visualization techniques to understand the incident. |  |
| 4 | Review | Review what was accomplished. Also discuss signs of a cyber event (malware infection) and possible ways to verify and isolate the event. |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |