This assignment guides students through three practical scenarios, each designed to address cybersecurity challenges using Python, Bash, and PowerShell. By leveraging Regex across multiple scripting languages, students will develop essential skills in log analysis, data sanitization, and threat detection.

To receive full credit, ensure your scripts are properly commented at the top and throughout, and include screenshots of your script outputs where requested in the lab instructions.

**NOTE: Be sure that you change your PowerShell & Bash script files extension to .txt so it will be accepted by BrightSpace.**

**Submission Requirements:**

* Submit the following through Brightspace:
  + Tool Dev 5 script files
  + The Week 8 - Tool Development 5 (**this document**) with all required screenshots.
  + The link/screenshot to/of your GitHub repository on the Tool Development 5 document showing this week’s script files pushed to the repository.

**Scenario 1 Script Output 1 Screenshot**

**A black screen with white text

Description automatically generated**

**Scenario 2 Script Output & Log Content Screenshots**

**A black background with white text

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**Scenario 3 Script Output Screenshot**

**A screenshot of a computer program

Description automatically generated**

**GitHub Repository Link or Screenshot of the files (on GitHub) https://github.com/hyamout/ISS212-Yamout**