Skill Assessment Test for Cyber Analytic Engineer

A. Automation Scripting

1. Provide a script to automate the extraction of IP addresses, URLs and hashes from the following cyber threat report.

   "Opsec Mistakes Reveal COBALT MIRAGE Threat Actors"
   (https://www.secureworks.com/blog/opsec-mistakes-reveal-cobalt-mirage-threat-actors)

   You can use any open source tools and library to help with the extraction.

2. With the domains extracted, develop a python script to extract WHOIS information for each domain. The output should be in a CSV file. You can use any open source library to develop the python script.

B. Cyber Threat Analysis

Provide a write-up for the following.

1. From the extracted IOCs, outline the type of enrichments that can facilitate cyber threat investigation.

2. How would you surface potentially unknown IOCs from the list of IOCs in the report?

C. Analytics Development

1. Design an algorithm to shortlist IPs that could be running reconnaissance activities against an enterprise web server. State any assumption you make in your design. Use the dataset in the following link to develop a prototype of the algorithm.

   https://www.secrepo.com/maccdc2012/http.log.gz