|  |
| --- |
| Cybersecurity |
| Module 19 Challenge Submission File |

## Let’s Go Splunking!

Make a copy of this document to work in, and then respond to each question below the prompt. Save and submit this completed file as your Challenge deliverable.

### Step 1: The Need for Speed

1. Based on the report you created, what is the approximate date and time of the attack?

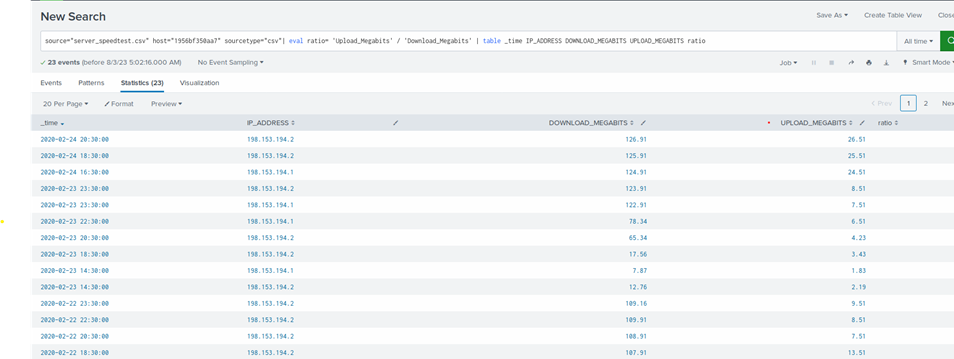
|  |
| --- |
| The Date and time of the attack was 2020-02-23 14:30:00 |

1. How long did it take your systems to recover?

|  |
| --- |
| The attack took for about 8 hours from 14:30:00 -22:30:00 |

Provide a screenshot of your report:

|  |
| --- |
|  |



### Step 2: Are We Vulnerable?

Provide a screenshot of your report:

|  |
| --- |
| [Place screenshot here] |

Provide a screenshot showing that the alert has been created:

|  |
| --- |
|  |

### Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

|  |
| --- |
| The Brute force attack occurred between Feb 21, 2020, 9:00 am – 1:30pm |

1. Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring:

|  |
| --- |
| Baseline would 15-30 counts per hour and Anything above 30 count would be considered as brute force attack |

1. Provide a screenshot showing that the alert has been created:

|  |
| --- |
|  |

A screenshot of a computer

Description automatically generated

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.