| 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?

| According to the report, the attack likely occurred on February 23, 2020, at 2:30 PM, as evidenced by a significant drop in download speed from 109.16 Mbps to 7.87 Mbps at that time. |
| --- |

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

| The systems appeared to recover at 10:30 PM, taking a total of around nine hours to restore from 2:30 PM to 10:30 PM on the same day. |
| --- |

Provide a screenshot of your report:

| source="server\_speedtest.csv" | eval ratio = 'UPLOAD\_MEGABITS' / 'DOWNLOAD\_MEGABITS' | table \_time IP\_ADDRESS DOWNLOAD\_MEGABITS UPLOAD\_MEGABITS ratio |
| --- |

### Step 2: Are We Vulnerable?

Provide a screenshot of your report:

| source="nessus\_logs.csv" dest\_ip"10.11.36.23" severity="critical" |
| --- |

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 attack occurred between 9:00 AM and 1:00 PM on February 21, 2020. |
| --- |

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

| Normal activity for failed login attempts typically fluctuates between six (6) and approximately 20 attempts per hour. During the hours of the attack, the number of failed login attempts surged to 124, 101, 121, 95, and 123 per hour. A baseline for normal failed login attempts might be set at 25 per hour, with a threshold of 50 attempts per hour triggering an alert. |
| --- |

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

|  |
| --- |

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