Kia Johnson

Unit 18 Homework Solution Guide: Lets go Splunking!

Step 1: The Need for Speed

 Based on the report created, what is the approximate date and time of the attack?

\*The attack occurred 2/23/2020 at 2:30PM when the upload and download speeds dropped

 When did the system begin to recover?

\*System recovered 2/23/2020 at 8:30PM from the attack it took 6 hours to recovery.

 When did the network traffic flow appear to be normal?

\*Traffic appeared network traffic recovered around 11:30

Graphical user interface, application, email

Description automatically generated

Graphical user interface

Description automatically generated with low confidence

Graphical user interface, table

Description automatically generated

Step 2: Are We Vulnerable?

Graphical user interface, application

Description automatically generatedGraphical user interface, text, application

Description automatically generatedGraphical user interface, text, application

Description automatically generated

Step 3: Drawing the (base)line

Admin logins

When did the brute force attack occur?

The attack happened February 21 from 9:00AM-1:00PM. Having logins 30 to 50 bad logins indicate a brute force attack.

Graphical user interface, text, application

Description automatically generatedA screenshot of a computer

Description automatically generated with medium confidenceGraphical user interface, application, Word

Description automatically generatedGraphical user interface, text

Description automatically generated