Arctos Morei  
**Homework 18: Let’s Go Splunking!**

Step 1 – The Need For Speed

Graphical user interface, website

Description automatically generated

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

Sun, Feb 23, 2020 at around 2:30pm

How long did it take your systems to recover?  
Recovered at 11:30pm, so approx. 9 hours.

Step 2 – Are We Vulnerable?



Graphical user interface, text, application, email

Description automatically generatedGraphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Step 3: Drawing the (base)line

When did the brute force attack occur?

Friday, Feb 21, 2020 from 8am – 2pm

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

In general, I’m seeing 0 – 25 failed login attempts as a baseline. Therefore, we’ll make the threshold 30.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated