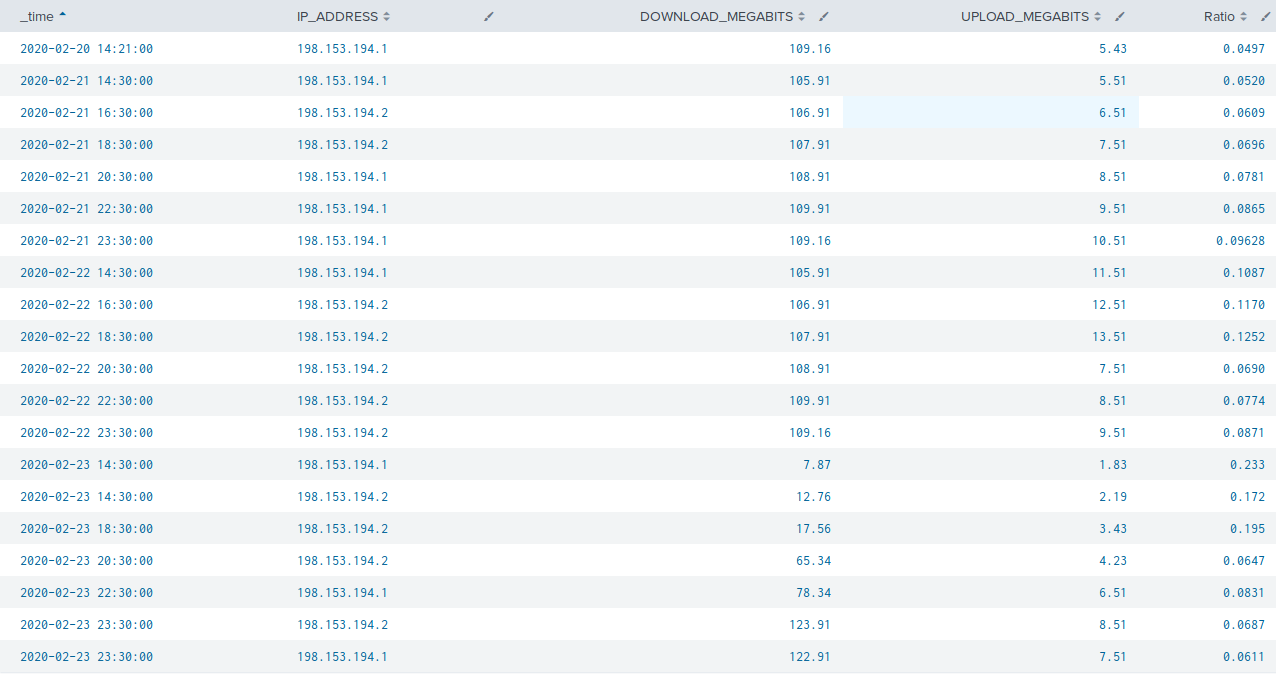
**Vandalay Industries**

Log analysis, automation and alerting.

**Task 1.** Analyze DDOS attack log and determine the impact that the DDOS attack had on download and upload speed. Create an additional field to calculate the ratio of the upload speed to the download speed.

Screenshot 1:

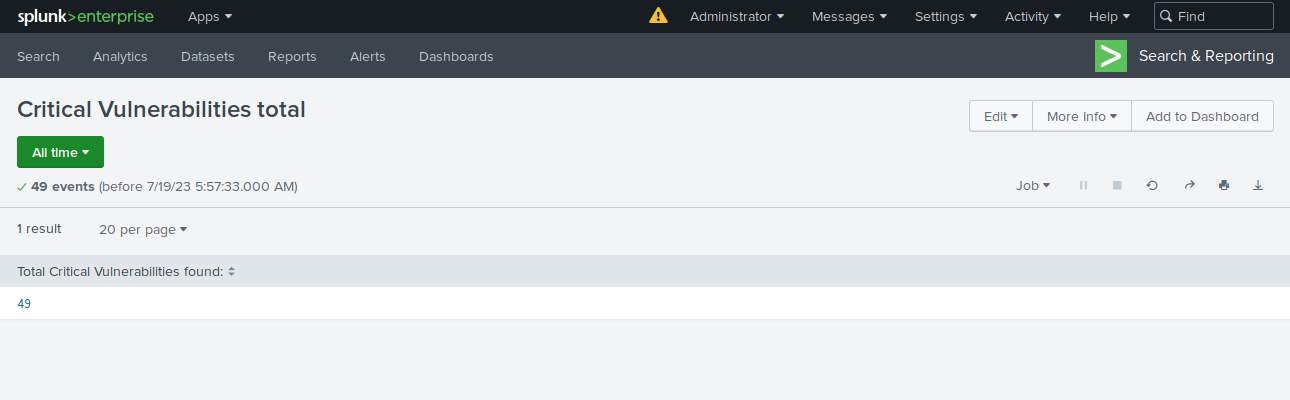


As you may see the attack took place 23/02/2020 around 2 pm. Local time. Complete recovery of speed took about 8 hours. During the attack the ratio between download and upload speed was 0.233 while in normal conditions it fluctuated between 0.050 and 0.100.

**Task 2**. Analyze vulnerability log from Nessus scan and determine steps for vulnerability control.

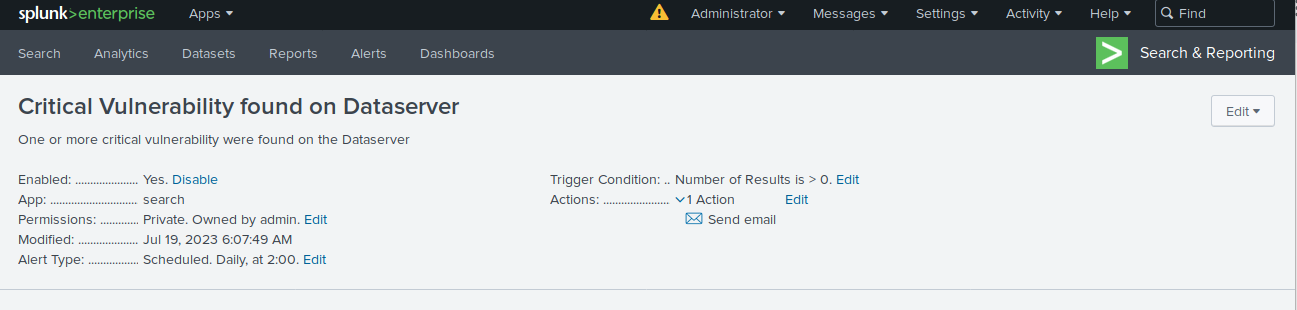
Provided log showed 49 critical vulnerabilities found on the database server. All of them needs to be eliminated as soon as possible.

Screenshot 2:



To keep continuous control on system health we created an alert that on a daily basis monitors Nessus logs and sends an email to [soc@vandanay.com](mailto:soc@vandanay.com) in the event when a new critical vulnerability will be discovered.

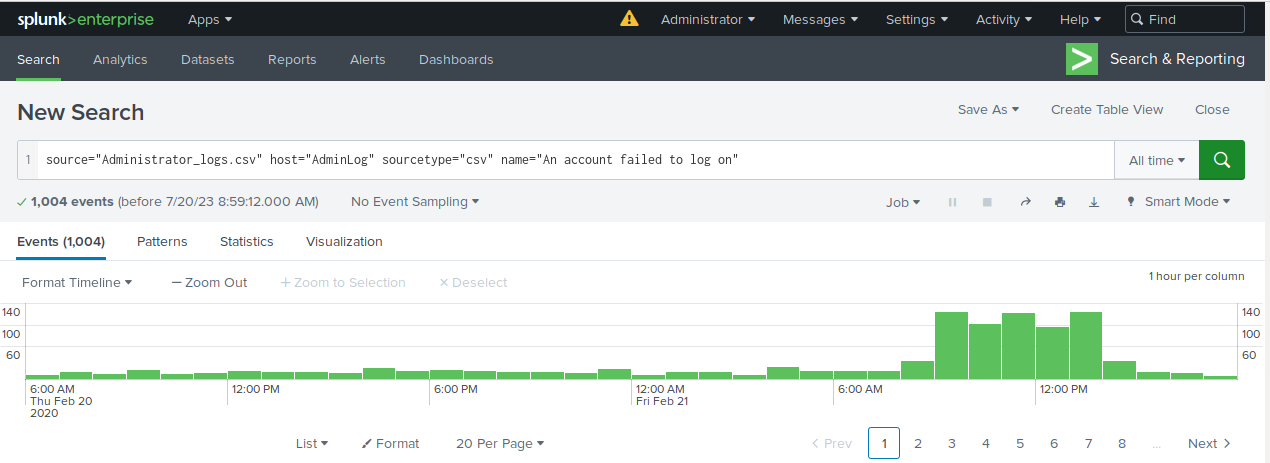
Screenshot 3:



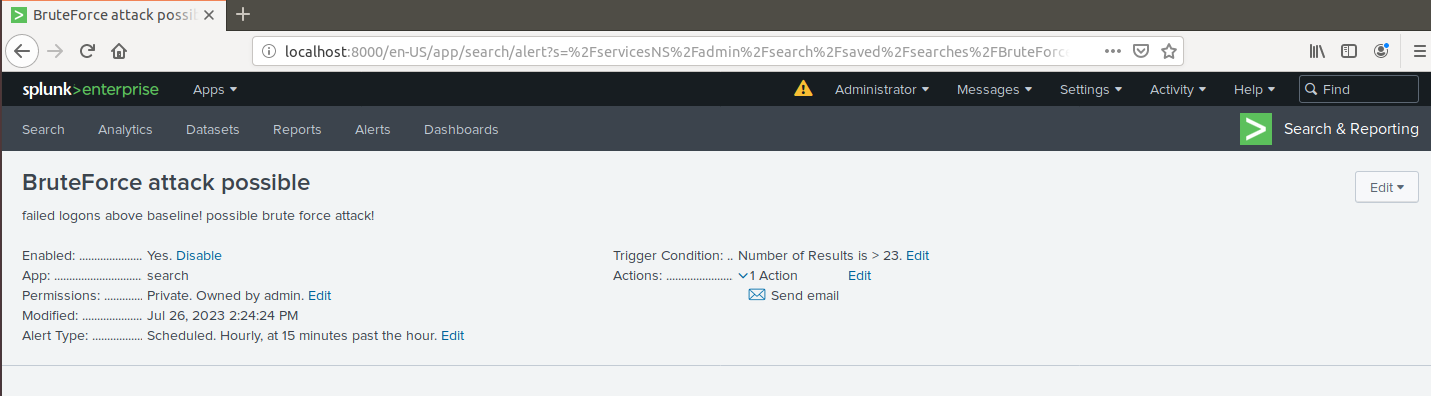
**Task 3.** Analyze a brute-force attack log, set a baseline and create an alert for early responding to possible future brute force attacks,

Presented log file showed the following findings:

The attack took place between 8 am and 3 pm on February 21 2020. As visible on the following screenshot there was a sharp increase in “Failed to logon” attempts in this time. Totally there were 1004 failed attempts recorded during two days - 20 and 21 of February. But looking inside hourly bars it was discovered that from 8 am and till 3 pm 21st of February there were up to 124 events per hour while on an average day there were no more than 23 records per hour.



Considering the above I decided to establish the baseline of 23 failed attempts per hour and create an alarm triggering if failed attempt count will exceed the baseline. The alarm will send an email to [SOC@vandalay.com](mailto:SOC@vandalay.com)



Signed:

Dmytro Goncharov