**Splunk questions**

1.How many successful events occurred?

**status=200 – 34282**

2.How many failed events occurred?

**status!=200 – 5250**

3.Which day had the most successful events?

**status=200 – April 21, 2014**

4.Which day had the most failed events?

**status!=200 – April 20, 2014**

5.How many purchase attempts were made?

**action=purchase – 5737**

6.Which day had the most purchase attempts?

**action=purchase – April 21, 2014**

7.How many successful purchases were made?

**action=purchase status=200 – 5224**

8.How many unsuccessful purchases were made?

**action=purchase status!=200 – 513**

9.Which log had the most successful events?

**status=200 | top limit=10 source – www1/access.log**

10.Which log had the most failed events?

**status!=200 | top limit=10 source – www1/access.log**

**Access log**

11.What IP address made the most purchases on Strategy games using Mozilla browser?

**action=purchase "categoryid=strategy" "Mozilla" | top limit=100 clientip – 128.241.220.82**

12.How many POST requests were made from google.com on WC-SH-G04 item?

**post "google" "productid=wc-sh-g04" – 29**

13.Which day was the third most successful day for Arcade games in sell?

**"categoryid=arcade" action=purchase – April 24, 2014**

**Secure log**

14.What is the most secure date in terms of fewer failed passwords?

**source="c:\buttercup.zip:.\buttercup/www1/secure.log" "failed" password – April 19, 2014**

15.What IP address was used the most for failed password for root?

**???**

16.How many errors have occurred using a Chrome browser?

**chrome AND error – 98**

17. For the www2/access.log how many events are there by a Mozilla browser and a GET method request?

**source="\*www2/access.log" "mozilla" AND method=GET – 7,669**

18.For the www1/access.log, in which day were the most strategy games sold?

**source="\*www1/access.log" "categoryid=strategy" action=purchase – April 24, 2014**

19. What is the number of accesses for POST from any IP address which starts with 198?

**post | regex \_raw="198\.\d{1,3}\.\d{1,3}\.\d{1,3}" – 401**