1 Splunk Tutorial 1

Using Splunk at https://asecuritysite.com:8443 determine the following. You will be allocated a login.

Demo: https://www.youtube.com/watch?v=bOQmd6B8jGo

1.1 Introduction to Splunk

Requirement	Answer
What is the start date of the log?	
How many log events are in *mailsv/secure.log?	
How many log events are in *www1/access.log?	
How many log events are in *www1/secure.log?	
How many log events are in *www2/access.log?	
What is the first username in the security log that gave an incorrect password (Hint: failed password | reverse)?	
What is the first IP address in the security log that gave an incorrect password (Hint: failed password | reverse)?	
How many accesses were accessed by a "Chrome" browser and a "GET" method request (Hint - "chrome" AND method=GET)?	
How many accesses were accessed by a "Chrome" browser or a "GET" method request (Hint - "chrome" OR method=GET)?	
How many accesses were accessed by a "Chrome" browser and a "POST" method request (Hint - "chrome" AND method=POST)?	
How many accesses were access by a "Chrome" browser or a "POST" method request (Hint - "chrome" OR method=POST)?	
When was the peak accesses by a "Chrome" browser or a "POST" method request (Hint - "chrome" OR method=POST)?	
How many accesses are there from a Safari browser (Hint: "safari")?	
How many accesses are there from a Chrome browser (Hint: "chrome")?	

How many accesses are there from a Mozilla browser (Hint: "mozilla")?	
On what day is there most activity in the secure logs (Hint: sourcetype=secure*)?	
For the access.log from www1, which is the most popular HTTP response value (Hint - source="*www1/access.log"| top limit=5 status)?	
For the access.log from www1, which is the second most popular HTTP response value (Hint = source="*www1/access.log"| top limit=5 status)?	
For the access.log from www1, which is the most popular IP address for accesses (Hint - source="*www1/access.log"| top limit=5 clientip)?	
For the access.log from www1, which is the second most popular IP address for accesses (Hint - source="*www1/access.log"| top limit=5 clientip)?	
For the access.log from www1, which is the most popular action (Hint - source="*www1/access.log"| top limit=5 action)?	
Refer to the Splunk analysis. For the access.log from www1, which is the second most popular action (source="*www1/access.log"| top limit=5 action)?	
For the access.log from www1, estimate the number of iPad accesses (Hint - source="*www1/access.log" ipad)?	
For the access.log from www1, what is the top refer domain (Hint - source=" *www1/access.log " | top limit=20 referer)?	
Which is the first time for a refer from google.com (Hint - source=" *www1/access.log" referer="http://www.google.com" | reverse)?	
Which is the IP address of the client which is first referred from google.com (source=" *www1/access.log" referer="http://www.google.com" | reverse)?	
Are there any successful accesses to signals.zip (Hint - signals.zip status=200)?	
Refer to the Splunk analysis for secure*.log. How many failed password attempts were there from 194.8.74.23 (Hint - sourcetype=secure* 194.8.74.23 failed)?	
Refer to the Splunk analysis for secure*.log. What day of the week had the most failed password attempts from 194.8.74.23 (Hint - sourcetype=secure* 194.8.74.23 failed)?	
What day had the most successful purchases (Hint - action=purchase status=200)?	

What day had the fewest purchases (Hint - action=purchase status=200)?	
What day had the most purchases which were not successfully processed (Hint - action=purchase status!=200)?	
How many STRATEGY games have been successfully purchased (Hint - categoryId=STRATEGY action=purchase status=200)?	
Refer to the Splunk analysis for access*.log. Which file access always produces a 404 return message: anna_nicole.html, productscreen.html, numa.html, cart.do and/or oldlink?	
How many ARCADE games have been successfully purchased (Hint - categoryId=ARCADE action=purchase status=200)?	
How many TEE games have been successfully purchased (Hint - categoryId=TEE action=purchase status=200)?	
How many SIMULATION games have been successfully purchased (Hint - categoryId=TEE action=purchase status=200)?	
How many SHOOTER games have been successfully purchased? (Hint - categoryId=SHOOTER action=purchase status=200)?	
Refer to the Splunk analysis for secure*.log. What day of the week had the least failed password attempts from 194.8.74.23 (Hint - failed password 194.8.74.23)?	
For an HTTP GET request, which is the most popular return code (Hint - sourcetype="access*" method="GET"| top limit=20 status)?	
For an HTTP GET request, which is the 2nd most popular return code (Hint - sourcetype="access*" method="GET"| top limit=20 status)?	
How many IP addresses have accessed the "passwords.pdf" file? What is/are the return HTTP status code(s) for these accesses?	

1.2 Test

Now perform the following test:

https://asecuritysite.com/tests/tests?sortby=siem