
ATTACK
DEFENSE
by PentesterAcademy

Name	Apache Log Analysis Basics II
URL	https://www.attackdefense.com/challengedetails?cid=139
Type	Forensics : Webserver Log Analysis

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

Question 1: List super-set of all HTTP request methods present in the logs.

Answer: GET , HEAD, POST, PUT

Solution:

Command: awk '{print $6}' apache_access.log | sort | uniq

```
student@attackdefense:~$ awk '{print $6}' apache_access.log | sort | uniq

"GET
"HEAD
"POST
"PUT
student@attackdefense:~$
```

Question 2: How many requests were made using protocol defined in RFC 1945?

Answer: 2061

Solution:

Command: awk '{print $8}' apache_access.log | sort | uniq -c

```
student@attackdefense:~$  awk '{print $8}' apache_access.log | sort | uniq -c
      1
   2061 HTTP/1.0"
   7938 HTTP/1.1"
student@attackdefense:~$
```

Question 3: How many requests were originated from Android Kitkat devices?

Answer: 35

Solution:

Command: awk -F\" '{print $6}' apache_access.log | grep -i android | sort | uniq -c | sort -fn

```
student@attackdefense:~$  awk -F\" '{print $6}' apache_access.log | grep -i android | sort | uniq -c | sort -fn
      4 Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0
     31 Mozilla/5.0 (Linux; Android 4.4.2; de-at; SAMSUNG GT-I9301I Build/KOT49H) AppleWebKit/537.36 (KHTML, like Gecko) Version/1.5 Chrome/28.
0.1500.94 Mobile Safari/537.36
     31 Mozilla/5.0 (Linux; Android 5.0.2; SAMSUNG SM-T530 Build/LRX22G) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/3.2 Chrome/38.0.
2125.102 Safari/537.36
student@attackdefense:~$
```

Question 4: How many POST requests were made for "/administrator/index.php" page?

Answer: 3583

Solution:

Command: awk -F\" '{print $2}' apache_access.log | grep administrator | grep POST | sort | uniq -c | sort -fn

```
student@attackdefense:~$ awk -F\" '{print $2}' apache_access.log | grep administrator | grep POST | sort | uniq -c | sort -fn
    962 POST /administrator/index.php HTTP/1.0
   2621 POST /administrator/index.php HTTP/1.1
student@attackdefense:~$
```

Question 5: Which browser was used to make GET requests to the server between 03:40 and 03:49 on 13th December 2015?

Answer: Firefox/34.0

Solution:

Command: grep "13/Dec/2015:03:4" apache_access.log | grep GET

```
student@attackdefense:~$ grep "13/Dec/2015:03:4" apache_access.log  | grep GET
146.120.107.98 - - [13/Dec/2015:03:44:58 +0100] "GET /administrator/ HTTP/1.1" 200 4263 "-" "Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/201001
01 Firefox/34.0" "-"
178.204.13.65 - - [13/Dec/2015:03:46:53 +0100] "GET /administrator/ HTTP/1.1" 200 4263 "-" "Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/2010010
1 Firefox/34.0" "-"
student@attackdefense:~$
```

Question 6:. How many requests were made by Google's crawling bots?

Answer: 105

Solution:

Command: awk -F\" '{print $6}' apache_access.log | grep Googlebot | wc -l

```
student@attackdefense:~$ awk -F\" '{print $6}' apache_access.log | grep Googlebot | wc -l
105
student@attackdefense:~$
```

Question 7: Which image was fetched from the server second most time?

Answer: almhuette_raith_01.jpg

Solution:

Command: awk -F\" '{print $2}' apache_access.log | grep ".jpg" | cut -d " " -f2 | sort | uniq -c | sort -k1 -n

```
student@attackdefense:~$ awk -F\" '{print $2}' apache_access.log | grep ".jpg" | cut -d " " -f2 | sort | uniq -c | sort -k1 -n | tail -5
     55 /images/stories/slideshow/almhuette_raith_03.jpg
     56 /images/stories/slideshow/almhuette_raith_04.jpg
     56 /images/stories/slideshow/almhuette_raith_05.jpg
     57 /images/stories/slideshow/almhuette_raith_01.jpg
     58 /images/stories/slideshow/almhuette_raith_02.jpg
student@attackdefense:~$
```