ATTACK DEFENSE

by PentesterAcademy

Name	Apache Log Analysis Basics
URL	https://www.attackdefense.com/challengedetails?cid=103
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.

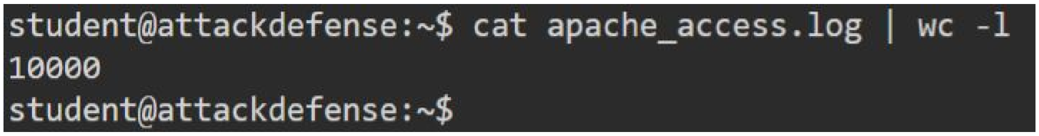
Question 1: How many logs are present in the given log file?

Answer: 10000

Solution:

Count the total number of logs in the log file.

Command: cat apache_access.log | wc -l



```
student@attackdefense:~$ cat apache_access.log | wc -l
10000
student@attackdefense:~$
```

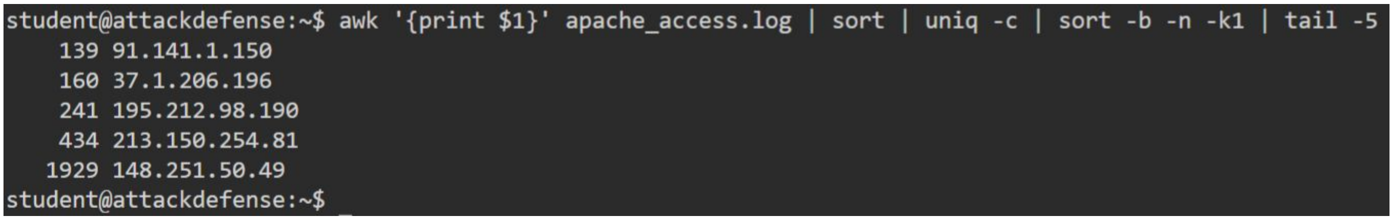
Question 2: Print top 5 clients IPs by number of requests made

Answer:

- 91.141.1.150
- 37.1.206.196
- 195.212.98.190
- 213.150.254.81
- 148.251.50.49

Solution:

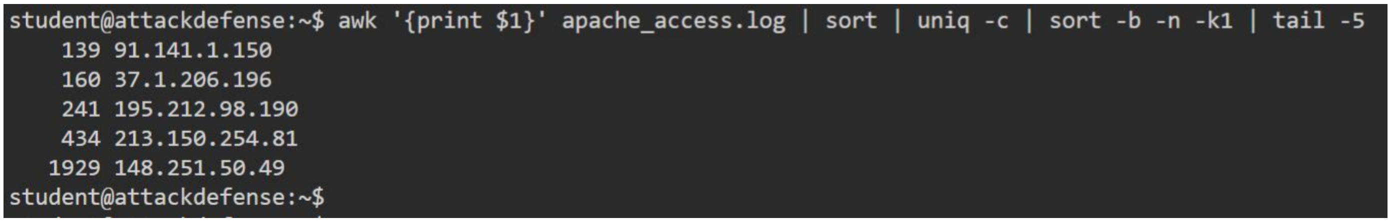
Command: awk '{print $1}' apache_access.log | sort | uniq -c | sort -b -n -k1 | tail -5



```
student@attackdefense:~$ awk '{print $1}' apache_access.log | sort | uniq -c | sort -b -n -k1 | tail -5
    139 91.141.1.150
    160 37.1.206.196
    241 195.212.98.190
    434 213.150.254.81
   1929 148.251.50.49
student@attackdefense:~$ _
```

Another alternate solution can be

Command: awk '{print $1}' apache_access.log | sort | uniq -c | sort -b -n -k1



```
student@attackdefense:~$ awk '{print $1}' apache_access.log | sort | uniq -c | sort -b -n -k1 | tail -5
    139 91.141.1.150
    160 37.1.206.196
    241 195.212.98.190
    434 213.150.254.81
   1929 148.251.50.49
student@attackdefense:~$
```

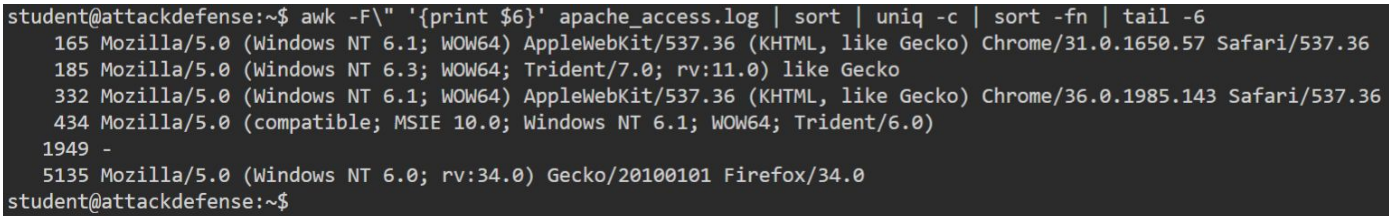
Question 3: Print top 5 user agents by number of requests logged by the server.

Answer:

- Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.57 Safari/537.36
- Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
- Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.143 Safari/537.36
- Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
- Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0\

Solution:

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



```
student@attackdefense:~$ awk -F\" '{print $6}' apache_access.log | sort | uniq -c | sort -fn | tail -6
    165 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.57 Safari/537.36
    185 Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
    332 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.143 Safari/537.36
    434 Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
   1949 -
   5135 Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0
student@attackdefense:~$
```

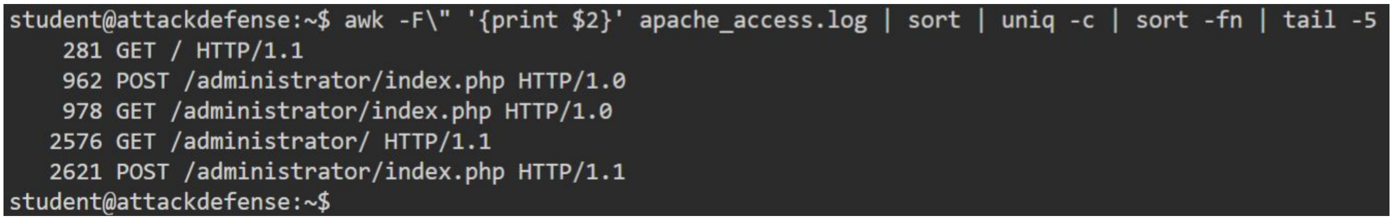
Question 4: Print top 5 requested URLs by requests (Request method and URL combined).

Answer:

- GET / HTTP/1.1
- POST /administrator/index.php HTTP/1.0
- GET /administrator/index.php HTTP/1.0
- GET /administrator/ HTTP/1.1
- POST /administrator/index.php HTTP/1.1

Solution:

Command: awk -F\" '{print $2}' apache_access.log | sort | uniq -c | sort -fn | tail -5



```
student@attackdefense:~$ awk -F\" '{print $2}' apache_access.log | sort | uniq -c | sort -fn | tail -5
    281 GET / HTTP/1.1
    962 POST /administrator/index.php HTTP/1.0
    978 GET /administrator/index.php HTTP/1.0
   2576 GET /administrator/ HTTP/1.1
   2621 POST /administrator/index.php HTTP/1.1
student@attackdefense:~$
```

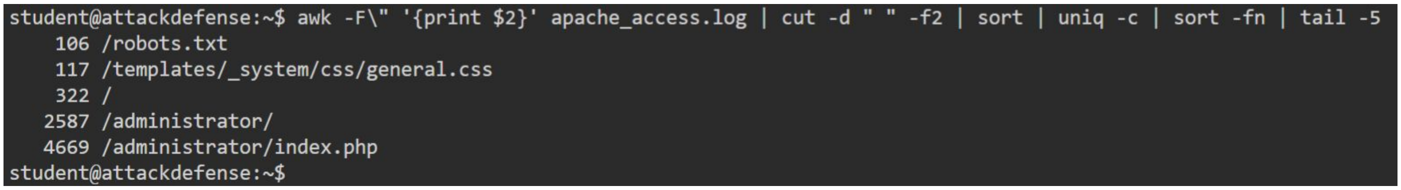
Question 5: Print top 5 requested URLs by visits (No need to consider request method).

Answer:

- /robots.txt
- /templates/_system/css/general.css
- /
- /administrator/
- /administrator/index.php

Solution:

Command: awk -F\" '{print $2}' apache_access.log | cut -d " " -f2 | sort | uniq -c | sort -fn | tail -5

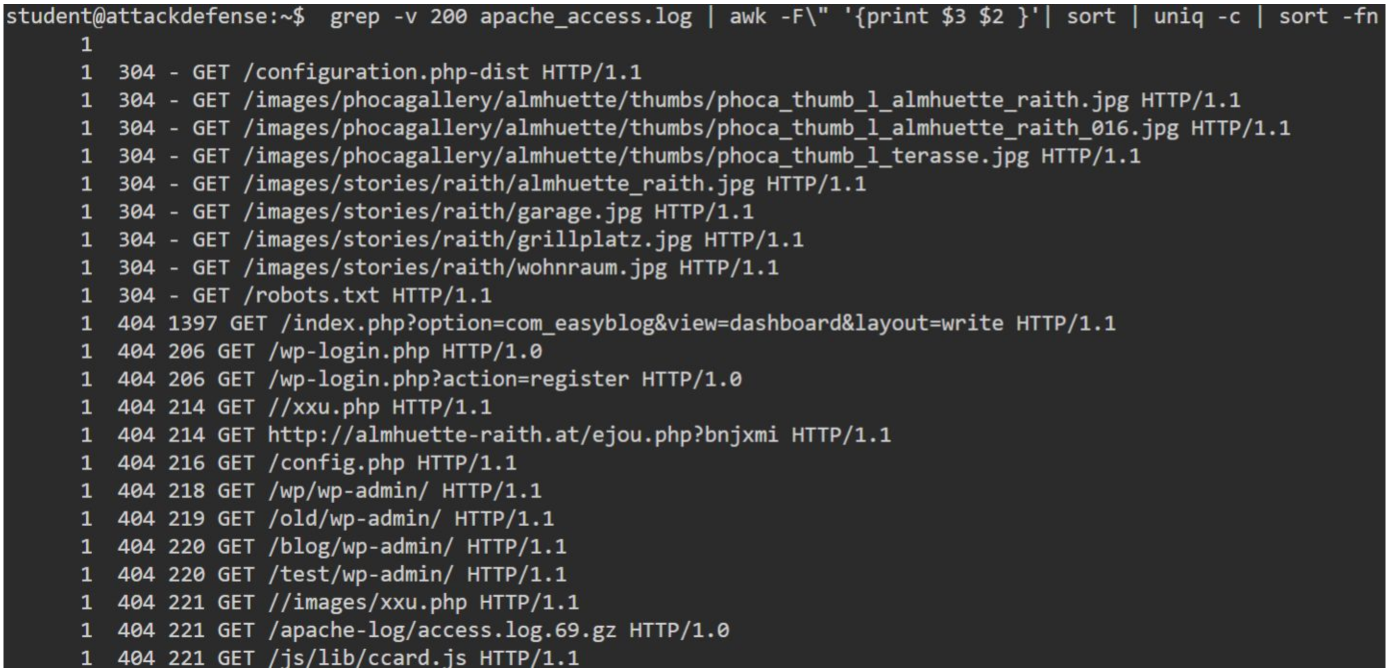


```
student@attackdefense:~$ awk -F\" '{print $2}' apache_access.log | cut -d " " -f2 | sort | uniq -c | sort -fn | tail -5
    106 /robots.txt
    117 /templates/_system/css/general.css
    322 /
   2587 /administrator/
   4669 /administrator/index.php
student@attackdefense:~$
```

Question 6: Print all URLs with non OK response status.

Solution:

Command: grep -v 200 apache_access.log | awk -F\" '{print $3 $2 }'| sort | uniq -c | sort -fn

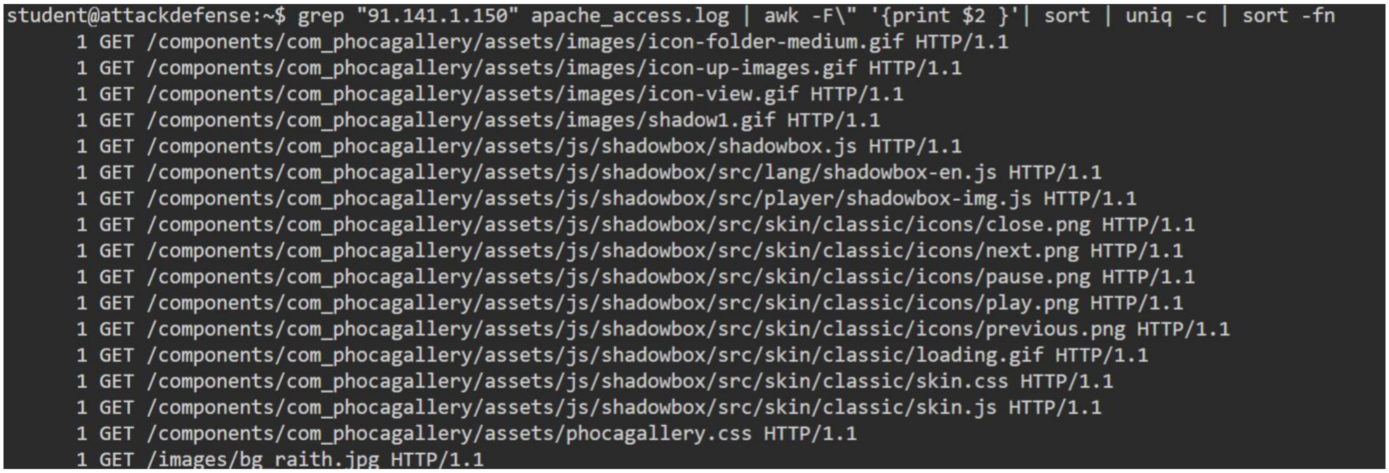


```
student@attackdefense:~$  grep -v 200 apache_access.log | awk -F\" '{print $3 $2 }'| sort | uniq -c | sort -fn
      1
      1  304 - GET /configuration.php-dist HTTP/1.1
      1  304 - GET /images/phocagallery/almhuette/thumbs/phoca_thumb_l_almhuette_raith.jpg HTTP/1.1
      1  304 - GET /images/phocagallery/almhuette/thumbs/phoca_thumb_l_almhuette_raith_016.jpg HTTP/1.1
      1  304 - GET /images/phocagallery/almhuette/thumbs/phoca_thumb_l_terasse.jpg HTTP/1.1
      1  304 - GET /images/stories/raith/almhuette_raith.jpg HTTP/1.1
      1  304 - GET /images/stories/raith/garage.jpg HTTP/1.1
      1  304 - GET /images/stories/raith/grillplatz.jpg HTTP/1.1
      1  304 - GET /images/stories/raith/wohnraum.jpg HTTP/1.1
      1  304 - GET /robots.txt HTTP/1.1
      1  404 1397 GET /index.php?option=com_easyblog&view=dashboard&layout=write HTTP/1.1
      1  404 206 GET /wp-login.php HTTP/1.0
      1  404 206 GET /wp-login.php?action=register HTTP/1.0
      1  404 214 GET //xxu.php HTTP/1.1
      1  404 214 GET http://almhuette-raith.at/ejou.php?bnjxmi HTTP/1.1
      1  404 216 GET /config.php HTTP/1.1
      1  404 218 GET /wp/wp-admin/ HTTP/1.1
      1  404 219 GET /old/wp-admin/ HTTP/1.1
      1  404 220 GET /blog/wp-admin/ HTTP/1.1
      1  404 220 GET /test/wp-admin/ HTTP/1.1
      1  404 221 GET //images/xxu.php HTTP/1.1
      1  404 221 GET /apache-log/access.log.69.gz HTTP/1.0
      1  404 221 GET /js/lib/ccard.js HTTP/1.1
```

Question 7: Print all the URLs accessed by client IP 91.141.1.150, in descending order by number of times URL was accessed.

Solution:

Command: grep "91.141.1.150" apache_access.log | awk -F\" '{print $2 }'| sort | uniq -c | sort -fn



```
student@attackdefense:~$ grep "91.141.1.150" apache_access.log | awk -F\" '{print $2 }'| sort | uniq -c | sort -fn
      1 GET /components/com_phocagallery/assets/images/icon-folder-medium.gif HTTP/1.1
      1 GET /components/com_phocagallery/assets/images/icon-up-images.gif HTTP/1.1
      1 GET /components/com_phocagallery/assets/images/icon-view.gif HTTP/1.1
      1 GET /components/com_phocagallery/assets/images/shadow1.gif HTTP/1.1
      1 GET /components/com_phocagallery/assets/js/shadowbox/shadowbox.js HTTP/1.1
      1 GET /components/com_phocagallery/assets/js/shadowbox/src/lang/shadowbox-en.js HTTP/1.1
      1 GET /components/com_phocagallery/assets/js/shadowbox/src/player/shadowbox-img.js HTTP/1.1
      1 GET /components/com_phocagallery/assets/js/shadowbox/src/skin/classic/icons/close.png HTTP/1.1
      1 GET /components/com_phocagallery/assets/js/shadowbox/src/skin/classic/icons/next.png HTTP/1.1
      1 GET /components/com_phocagallery/assets/js/shadowbox/src/skin/classic/icons/pause.png HTTP/1.1
      1 GET /components/com_phocagallery/assets/js/shadowbox/src/skin/classic/icons/play.png HTTP/1.1
      1 GET /components/com_phocagallery/assets/js/shadowbox/src/skin/classic/icons/previous.png HTTP/1.1
      1 GET /components/com_phocagallery/assets/js/shadowbox/src/skin/classic/loading.gif HTTP/1.1
      1 GET /components/com_phocagallery/assets/js/shadowbox/src/skin/classic/skin.css HTTP/1.1
      1 GET /components/com_phocagallery/assets/js/shadowbox/src/skin/classic/skin.js HTTP/1.1
      1 GET /components/com_phocagallery/assets/phocagallery.css HTTP/1.1
      1 GET /images/bg_raith.jpg HTTP/1.1
```