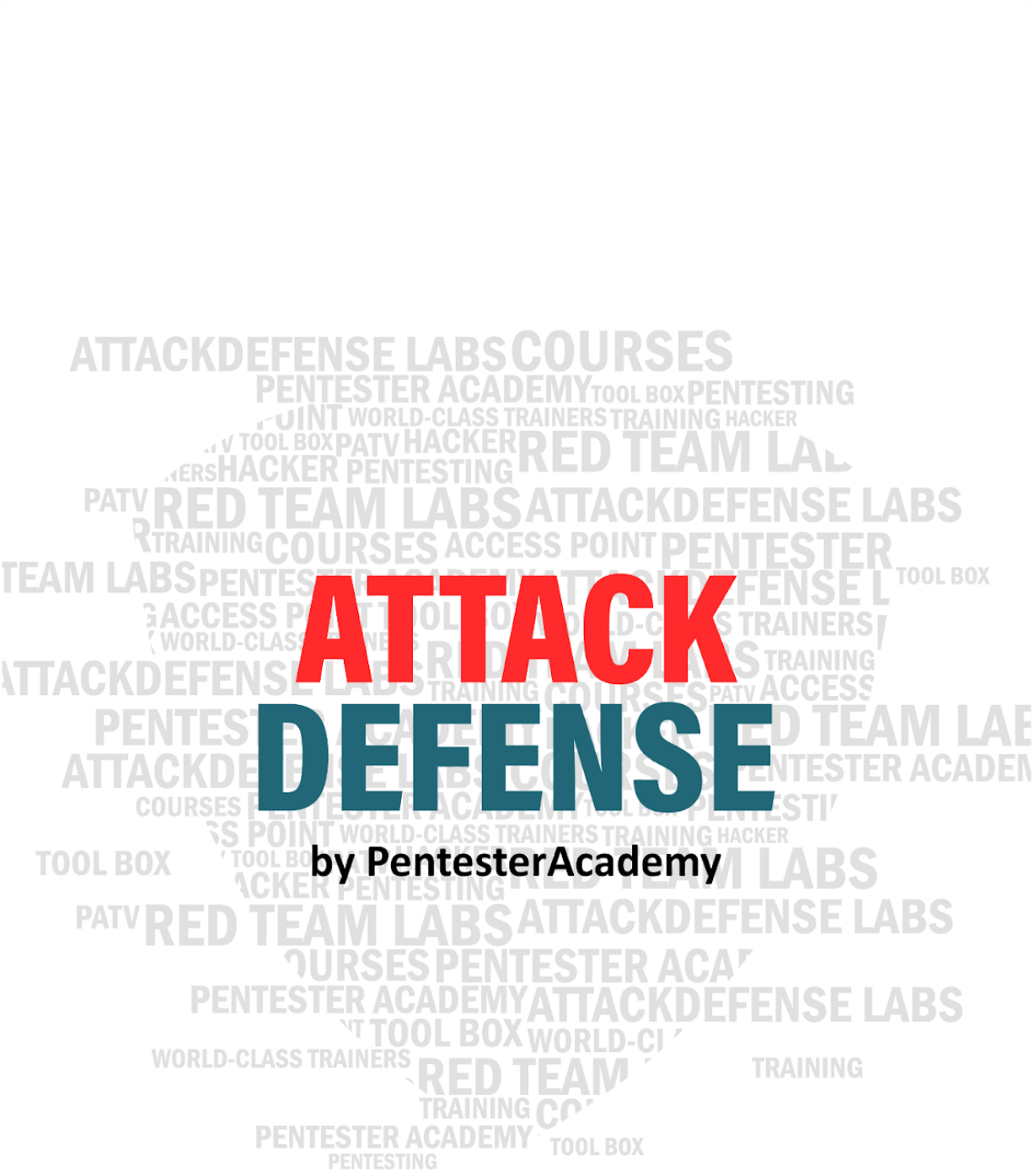
ATTACK
DEFENSE
by PentesterAcademy

Name	Text File Analysis
URL	https://attackdefense.com/challengedetails?cid=1808
Type	Beginner Skills : Linux For Pentesters

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. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Learn about text file analysis and manipulation by doing the following activities on apache_access.log file. The file is present in the home directory of the student user.

1. Check the contents of the file.
2. Print first 10 lines of the file
3. Print last 10 lines of the file
4. Print the lines containing the text string “jp_hotel".
5. How many lines contains the text string “jp_hotel"?
6. How many lines doesn’t contain the text string “css"?
7. Print only the first column for the last 5 lines using cut utility.
8. Print timestamp column for last 5 lines using cut utility.
9. Print only IPs from the file using awk utility.
10. Print only sorted IPs (ascending order) from the file.
11. Print only unique IPs from the file.
12. Print the last 5 lines and replace the space character (' ') with underscore character ('_') using tr utility.
13. Create a CSV file from the log file using tr utility.
14. Replace all occurrences of string 'iPad' with 'Apple iPad' in the file using sed utility.

Solution:

Check the contents of the working directory.

Command: ls -l

```
student@attackdefense:~$ ls -l
total 16
-rw-r--r-- 1 student student 14129 Apr  8 08:05 apache_access.log
student@attackdefense:~$
```

apache_access.log file is present in the directory.

Q 1. Check the contents of the file.

There are multiple ways to check the contents of the file.

Using editors like vim and nano

Command: vim apache_access.log

```
student@attackdefense:~$ vim apache_access.log
student@attackdefense:~$
```

Press “i” to enter the insertion mode. To exit, first press ESC and then type :q

```
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET / HTTP/1.1" 200 10479 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKi
t/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /modules/mod_bowslideshow/tmpl/css/bowslideshow.css HTTP/1.1" 200 1725 "http://www.almhuette-
raith.at/" "Mozilla/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/60
1.1" "-"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /media/system/js/caption.js HTTP/1.1" 200 1963 "http://www.almhuette-raith.at/" "Mozilla/5.0
(iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /templates/jp_hotel/js/moomenu.js HTTP/1.1" 200 4890 "http://www.almhuette-raith.at/" "Mozill
a/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /templates/_system/css/general.css HTTP/1.1" 404 239 "http://www.almhuette-raith.at/" "Mozill
a/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /templates/jp_hotel/css/menu.css HTTP/1.1" 200 1457 "http://www.almhuette-raith.at/" "Mozilla
/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-"
```

Using utilities like cat

Command: cat apache_access.log

```
student@attackdefense:~$ cat apache_access.log
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET / HTTP/1.1" 200 10479 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKi
t/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /modules/mod_bowslideshow/tmpl/css/bowslideshow.css HTTP/1.1" 200 1725 "http://www.almhuette-
raith.at/" "Mozilla/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/60
1.1" "-"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /media/system/js/caption.js HTTP/1.1" 200 1963 "http://www.almhuette-raith.at/" "Mozilla/5.0
(iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /templates/jp_hotel/js/moomenu.js HTTP/1.1" 200 4890 "http://www.almhuette-raith.at/" "Mozill
a/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /templates/_system/css/general.css HTTP/1.1" 404 239 "http://www.almhuette-raith.at/" "Mozill
a/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-"
```

Lengthy files are difficult to read with cat because most of the text . However in such cases, less command can be used.

Command: cat apache_access.log | less

Q 2. Print first 10 lines of the file

Command: cat apache_access.log | head -10

```
student@attackdefense:~$  cat apache_access.log | head -10
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET / HTTP/1.1" 200 10479 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKi
t/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /modules/mod_bowslideshow/tmpl/css/bowslideshow.css HTTP/1.1" 200 1725 "http://www.almhuette-
raith.at/" "Mozilla/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/60
1.1" "-"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /media/system/js/caption.js HTTP/1.1" 200 1963 "http://www.almhuette-raith.at/" "Mozilla/5.0
(iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /templates/jp_hotel/js/moomenu.js HTTP/1.1" 200 4890 "http://www.almhuette-raith.at/" "Mozill
a/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /templates/_system/css/general.css HTTP/1.1" 404 239 "http://www.almhuette-raith.at/" "Mozill
a/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /templates/jp_hotel/css/menu.css HTTP/1.1" 200 1457 "http://www.almhuette-raith.at/" "Mozilla
/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /templates/jp_hotel/css/suckerfish.css HTTP/1.1" 200 3465 "http://www.almhuette-raith.at/" "M
ozilla/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /templates/jp_hotel/css/template.css HTTP/1.1" 200 10004 "http://www.almhuette-raith.at/" "Mo
zilla/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /templates/jp_hotel/css/layout.css HTTP/1.1" 200 1801 "http://www.almhuette-raith.at/" "Mozil
la/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /modules/mod_bowslideshow/tmpl/js/sliderman.1.3.0.js HTTP/1.1" 200 33472 "http://www.almhuett
e-raith.at/" "Mozilla/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/
601.1" "-"
student@attackdefense:~$
```

Q 3. Print last 10 lines of the file

Command: cat apache_access.log | tail -10

```
student@attackdefense:~$  cat apache_access.log | tail -10
80.110.186.51 - - [21/Dec/2015:17:20:11 +0100] "GET /media/system/js/mootools.js HTTP/1.1" 200 74434 "http://www.almhuette-raith.at/" "Mozilla/5
.0 (iPad; CPU OS 9_1 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13B143 Safari/601.1" "-"
80.110.186.51 - - [21/Dec/2015:17:20:11 +0100] "GET /images/stories/raith/wohnraum.jpg HTTP/1.1" 200 43586 "http://www.almhuette-raith.at/" "Moz
illa/5.0 (iPad; CPU OS 9_1 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13B143 Safari/601.1" "-"
80.110.186.51 - - [21/Dec/2015:17:20:11 +0100] "GET /images/stories/slideshow/almhuette_raith_01.jpg HTTP/1.1" 200 88161 "http://www.almhuette-r
aith.at/" "Mozilla/5.0 (iPad; CPU OS 9_1 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13B143 Safari/601.1" "-"
80.110.186.51 - - [21/Dec/2015:17:20:11 +0100] "GET /images/stories/slideshow/almhuette_raith_07.jpg HTTP/1.1" 200 94861 "http://www.almhuette-r
aith.at/" "Mozilla/5.0 (iPad; CPU OS 9_1 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13B143 Safari/601.1" "-"
80.110.186.51 - - [21/Dec/2015:17:20:11 +0100] "GET /images/stories/slideshow/almhuette_raith_05.jpg HTTP/1.1" 200 77796 "http://www.almhuette-r
aith.at/" "Mozilla/5.0 (iPad; CPU OS 9_1 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13B143 Safari/601.1" "-"
80.110.186.51 - - [21/Dec/2015:17:20:11 +0100] "GET /images/stories/raith/almhuette_raith.jpg HTTP/1.1" 200 43300 "http://www.almhuette-raith.at
/" "Mozilla/5.0 (iPad; CPU OS 9_1 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13B143 Safari/601.1" "-"
80.110.186.51 - - [21/Dec/2015:17:20:11 +0100] "GET /images/stories/raith/almenland_logo.jpg HTTP/1.1" 200 21490 "http://www.almhuette-raith.at/
" "Mozilla/5.0 (iPad; CPU OS 9_1 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13B143 Safari/601.1" "-"
80.110.186.51 - - [21/Dec/2015:17:20:11 +0100] "GET /images/stories/raith/grillplatz.jpg HTTP/1.1" 200 55303 "http://www.almhuette-raith.at/" "M
ozilla/5.0 (iPad; CPU OS 9_1 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13B143 Safari/601.1" "-"
80.110.186.51 - - [21/Dec/2015:17:20:11 +0100] "GET /images/stories/slideshow/almhuette_raith_02.jpg HTTP/1.1" 200 62918 "http://www.almhuette-r
aith.at/" "Mozilla/5.0 (iPad; CPU OS 9_1 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13B143 Safari/601.1" "-"
80.110.186.51 - - [21/Dec/2015:17:20:12 +0100] "GET /images/stories/slideshow/almhuette_raith_06.jpg HTTP/1.1" 200 68977 "http://www.almhuette-r
aith.at/" "Mozilla/5.0 (iPad; CPU OS 9_1 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13B143 Safari/601.1" "-"
student@attackdefense:~$
```

Q 4. Print the lines containing the text string “jp_hotel".

Command: cat apache_access.log | grep "jp_hotel"

```
student@attackdefense:~$ cat apache_access.log | grep "jp_hotel"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /templates/jp_hotel/js/moomenu.js HTTP/1.1" 200 4890 "http://www.almhuette-raith.at/" "Mozill
a/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /templates/jp_hotel/css/menu.css HTTP/1.1" 200 1457 "http://www.almhuette-raith.at/" "Mozilla
/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /templates/jp_hotel/css/suckerfish.css HTTP/1.1" 200 3465 "http://www.almhuette-raith.at/" "M
ozilla/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /templates/jp_hotel/css/template.css HTTP/1.1" 200 10004 "http://www.almhuette-raith.at/" "Mo
zilla/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /templates/jp_hotel/css/layout.css HTTP/1.1" 200 1801 "http://www.almhuette-raith.at/" "Mozil
la/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-"
80.31.165.71 - - [21/Dec/2015:17:18:59 +0100] "GET /templates/jp_hotel/images/logo.jpg HTTP/1.1" 200 369 "http://www.almhuette-raith.at/" "Mozil
la/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-"
80.31.165.71 - - [21/Dec/2015:17:19:00 +0100] "GET /templates/jp_hotel/images/content_heading.gif HTTP/1.1" 200 69 "http://www.almhuette-raith.a
t/" "Mozilla/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1" "-
"
```

Q 5. How many lines contains the text string “jp_hotel"?

Command: cat apache_access.log | grep "jp_hotel" | wc -l

```
student@attackdefense:~$ cat apache_access.log | grep "jp_hotel" | wc -l
13
student@attackdefense:~$
```

Q 6. How many lines doesn't contain the text string "css"?

Command: cat apache_access.log | grep -v "css" | wc -l

```
student@attackdefense:~$ cat apache_access.log | grep -v "css" | wc -l
38
student@attackdefense:~$
```

Q 7. Print only the first column for the last 5 lines using cut utility.

Command: cat apache_access.log | tail -5 | cut -d " " -f1

```
student@attackdefense:~$ cat apache_access.log | tail -5 | cut -d " " -f1
80.110.186.51
80.110.186.51
80.110.186.51
80.110.186.51
80.110.186.51
student@attackdefense:~$
```

Q 8. Print timestamp column for last 5 lines using cut utility.

Command: cat apache_access.log | tail -5 | cut -d " " -f4 | cut -d "[" -f2

```
student@attackdefense:~$ cat apache_access.log | tail -5 | cut -d " " -f4 | cut -d "[" -f2
21/Dec/2015:17:20:11
21/Dec/2015:17:20:11
21/Dec/2015:17:20:11
21/Dec/2015:17:20:11
21/Dec/2015:17:20:12
student@attackdefense:~$
```

Q 9. Print only IPs from the file using awk utility.

Command: awk '{print $1}' apache_access.log

```
student@attackdefense:~$ awk '{print $1}' apache_access.log
80.31.165.71
80.31.165.71
80.31.165.71
80.31.165.71
80.31.165.71
80.31.165.71
80.31.165.71
80.31.165.71
```

Q 10. Print only sorted IPs (ascending order) from the file.

Command: awk '{print $1}' apache_access.log | sort

```
student@attackdefense:~$  awk '{print $1}' apache_access.log | sort
80.110.186.51
80.110.186.51
80.110.186.51
80.110.186.51
80.110.186.51
80.110.186.51
80.110.186.51
80.110.186.51
80.110.186.51
80.110.186.51
80.110.186.51
80.110.186.51
80.110.186.51
80.110.186.51
80.110.186.51
80.110.186.51
80.110.186.51
80.110.186.51
80.110.186.51
80.110.186.51
80.31.165.71
```

Q 11. Print only unique IPs from the file.

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

```
student@attackdefense:~$ awk '{print $1}' apache_access.log | sort | uniq -c
     20 80.110.186.51
     30 80.31.165.71
student@attackdefense:~$
```

Q 12. Print the last 5 lines and replace the space character (' ') with underscore character ('_') using tr utility.

Command: cat apache_access.log | tail -5 | tr ' ' '-'

```
student@attackdefense:~$ cat apache_access.log | tail -5 | tr ' ' '-'
80.110.186.51-----[21/Dec/2015:17:20:11-+0100]-"GET-/images/stories/raith/almhuette_raith.jpg-HTTP/1.1"-200-43300-"http://www.almhuette-raith.at
/"-"Mozilla/5.0-(iPad;-CPU-OS-9_1-like-Mac-OS-X)-AppleWebKit/601.1.46-(KHTML,-like-Gecko)-Version/9.0-Mobile/13B143-Safari/601.1"-"-"
80.110.186.51-----[21/Dec/2015:17:20:11-+0100]-"GET-/images/stories/raith/almenland_logo.jpg-HTTP/1.1"-200-21490-"http://www.almhuette-raith.at/
"-"Mozilla/5.0-(iPad;-CPU-OS-9_1-like-Mac-OS-X)-AppleWebKit/601.1.46-(KHTML,-like-Gecko)-Version/9.0-Mobile/13B143-Safari/601.1"-"-"
80.110.186.51-----[21/Dec/2015:17:20:11-+0100]-"GET-/images/stories/raith/grillplatz.jpg-HTTP/1.1"-200-55303-"http://www.almhuette-raith.at/"-"M
ozilla/5.0-(iPad;-CPU-OS-9_1-like-Mac-OS-X)-AppleWebKit/601.1.46-(KHTML,-like-Gecko)-Version/9.0-Mobile/13B143-Safari/601.1"-"-"
80.110.186.51-----[21/Dec/2015:17:20:11-+0100]-"GET-/images/stories/slideshow/almhuette_raith_02.jpg-HTTP/1.1"-200-62918-"http://www.almhuette-r
aith.at/"-"Mozilla/5.0-(iPad;-CPU-OS-9_1-like-Mac-OS-X)-AppleWebKit/601.1.46-(KHTML,-like-Gecko)-Version/9.0-Mobile/13B143-Safari/601.1"-"-"
80.110.186.51-----[21/Dec/2015:17:20:12-+0100]-"GET-/images/stories/slideshow/almhuette_raith_06.jpg-HTTP/1.1"-200-68977-"http://www.almhuette-r
aith.at/"-"Mozilla/5.0-(iPad;-CPU-OS-9_1-like-Mac-OS-X)-AppleWebKit/601.1.46-(KHTML,-like-Gecko)-Version/9.0-Mobile/13B143-Safari/601.1"-"-"
student@attackdefense:~$
```

Q 13. Create a CSV file from the log file using tr utility.

Command: cat apache_access.log | tr ' ' ',' > apache_access.csv

```
student@attackdefense:~$ cat apache_access.log | tr ' ' ',' > apache_access.csv
student@attackdefense:~$
```

Check the last 5 lines of the apache_access.csv file to verify the change.

Command: cat apache_access.csv | tail -5

```
student@attackdefense:~$ cat apache_access.log | tr ' ' ',' > apache_access.csv
student@attackdefense:~$
student@attackdefense:~$ cat apache_access.csv | head -5
80.31.165.71,-,-,[21/Dec/2015:17:18:59,+0100],"GET,/,HTTP/1.1",200,10479,"-","Mozilla/5.0,(iPhone;,CPU,iPhone,OS,9_0_2,like,Mac,OS,X),AppleWebKi
t/601.1.46,(KHTML,,like,Gecko),Version/9.0,Mobile/13A452,Safari/601.1","-"
80.31.165.71,-,-,[21/Dec/2015:17:18:59,+0100],"GET,/modules/mod_bowslideshow/tmpl/css/bowslideshow.css,HTTP/1.1",200,1725,"http://www.almhuette-
raith.at/","Mozilla/5.0,(iPhone;,CPU,iPhone,OS,9_0_2,like,Mac,OS,X),AppleWebKit/601.1.46,(KHTML,,like,Gecko),Version/9.0,Mobile/13A452,Safari/60
1.1","-"
80.31.165.71,-,-,[21/Dec/2015:17:18:59,+0100],"GET,/media/system/js/caption.js,HTTP/1.1",200,1963,"http://www.almhuette-raith.at/","Mozilla/5.0,
(iPhone;,CPU,iPhone,OS,9_0_2,like,Mac,OS,X),AppleWebKit/601.1.46,(KHTML,,like,Gecko),Version/9.0,Mobile/13A452,Safari/601.1","-"
80.31.165.71,-,-,[21/Dec/2015:17:18:59,+0100],"GET,/templates/jp_hotel/js/moomenu.js,HTTP/1.1",200,4890,"http://www.almhuette-raith.at/","Mozill
a/5.0,(iPhone;,CPU,iPhone,OS,9_0_2,like,Mac,OS,X),AppleWebKit/601.1.46,(KHTML,,like,Gecko),Version/9.0,Mobile/13A452,Safari/601.1","-"
80.31.165.71,-,-,[21/Dec/2015:17:18:59,+0100],"GET,/templates/_system/css/general.css,HTTP/1.1",404,239,"http://www.almhuette-raith.at/","Mozill
a/5.0,(iPhone;,CPU,iPhone,OS,9_0_2,like,Mac,OS,X),AppleWebKit/601.1.46,(KHTML,,like,Gecko),Version/9.0,Mobile/13A452,Safari/601.1","-"
student@attackdefense:~$
```

Q 14. Replace all occurrences of string 'iPad' with 'Apple iPad' in the file using sed utility.

List the lines containing string 'iPad'

Command: cat apache_access.log | grep "iPad"

```
student@attackdefense:~$ cat apache_access.log | grep "iPad"
80.110.186.51 - - [21/Dec/2015:17:20:11 +0100] "GET / HTTP/1.1" 200 10479 "http://booking.almenland.at/almenland/de/accommodation/detail/AT1/bde
6f5f7-f571-4d82-90cd-0046a09dfdc0/almh%C3%BCtte_raith?customHeader=true" "Mozilla/5.0 (iPad; CPU OS 9_1 like Mac OS X) AppleWebKit/601.1.46 (KHT
ML, like Gecko) Version/9.0 Mobile/13B143 Safari/601.1" "-"
80.110.186.51 - - [21/Dec/2015:17:20:11 +0100] "GET /modules/mod_bowslideshow/tmpl/css/bowslideshow.css HTTP/1.1" 200 1725 "http://www.almhuette
-raith.at/" "Mozilla/5.0 (iPad; CPU OS 9_1 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13B143 Safari/601.1" "-"
80.110.186.51 - - [21/Dec/2015:17:20:11 +0100] "GET /media/system/js/caption.js HTTP/1.1" 200 1963 "http://www.almhuette-raith.at/" "Mozilla/5.0
 (iPad; CPU OS 9_1 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13B143 Safari/601.1" "-"
```

Replace all occurrences

Command: sed -i 's/iPad/Apple iPad/g' apache_access.log

```
student@attackdefense:~$
student@attackdefense:~$ sed -i 's/iPad/Apple iPad/g' apache_access.log
student@attackdefense:~$
```

Again, list the lines containing string 'iPad' to confirm the change

Command: cat apache_access.log | grep "iPad"

```
student@attackdefense:~$ cat apache_access.log | grep "iPad"
80.110.186.51 - - [21/Dec/2015:17:20:11 +0100] "GET / HTTP/1.1" 200 10479 "http://booking.almenland.at/almenland/de/accommodation/detail/AT1/bde
6f5f7-f571-4d82-90cd-0046a09dfdc0/almh%C3%BCtte_raith?customHeader=true" "Mozilla/5.0 (Apple iPad; CPU OS 9_1 like Mac OS X) AppleWebKit/601.1.4
6 (KHTML, like Gecko) Version/9.0 Mobile/13B143 Safari/601.1" "-"
80.110.186.51 - - [21/Dec/2015:17:20:11 +0100] "GET /modules/mod_bowslideshow/tmpl/css/bowslideshow.css HTTP/1.1" 200 1725 "http://www.almhuette
-raith.at/" "Mozilla/5.0 (Apple iPad; CPU OS 9_1 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13B143 Safari/601.1"
 "-"
80.110.186.51 - - [21/Dec/2015:17:20:11 +0100] "GET /media/system/js/caption.js HTTP/1.1" 200 1963 "http://www.almhuette-raith.at/" "Mozilla/5.0
 (Apple iPad; CPU OS 9_1 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13B143 Safari/601.1" "-"
```

References:

- Apache_access.log source: http://www.almhuette-raith.at/apache-log/access.log