
ATTACK
DEFENSE
by PentesterAcademy

Name	Apache Error Log Analysis Basics
URL	https://www.attackdefense.com/challengedetails?cid=140
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 requests were made for non-existent pages?

Answer: 229112

Solution:

Command: cat error.log | grep " File does not exist" | cut -d "]" -f4 | cut -d ":" -f2 | wc -l

```
student@attackdefense:~$ cat error.log | grep " File does not exist" | cut -d "]" -f4 | cut -d ":" -f2 | wc -l
229112
student@attackdefense:~$
```

Question 2: How many unique usernames were used to bruteforce the basic authentication protected page?

Answer: 75

Solution:

Command: cat error.log | cut -d "]" -f4 | cut -d ":" -f1 | grep user | cut -d " " -f3 | sort | uniq | wc -l

```
student@attackdefense:~$ cat error.log | cut -d "]" -f4 | cut -d ":" -f1 | grep user | cut -d " " -f3 | sort | uniq | wc -l
75
student@attackdefense:~$
student@attackdefense:~$
```

Question 3: Create a list of all unique usernames used to bruteforce the basic authentication protected page?

Command: cat error.log | cut -d "]" -f4 | cut -d ":" -f1 | grep user | cut -d " " -f3 | sort | uniq > list

```
student@attackdefense:~$ cat error.log | cut -d "]" -f4 | cut -d ":" -f1 | grep user | cut -d " " -f3 | sort | uniq > list
student@attackdefense:~$ cat list

1502
ADMIN
Admin
Administrator
AdvWebadmin
Bobo
Cisco
Coco
Flo
Jetform
Joe
LDAP_Anonymous
Manager
Moe
Polycom
QCC
Root
```

Question 4: How many requests were made to perform directory traversal or Local File Inclusion attack? And, also list the files which attacker was trying to access.

Answer: 15
boot.ini, sam, config.dat, passwd, win.ini, vmInventory.xml, dvr2.ini, shadow

Solution:

Command: grep "/\.\./\.\./" error.log

```
student@attackdefense:~$  grep "/\.\./\.\./" error.log
[Wed Jun 20 09:17:28 2018] [error] [client 91.218.225.68] Invalid URI in request GET /../../../../../../../../../boot.ini HTTP/1.1
[Wed Jun 20 09:17:28 2018] [error] [client 91.218.225.68] Invalid URI in request GET /../../../../winnt/repair/sam._ HTTP/1.1
[Wed Jun 20 09:17:29 2018] [error] [client 91.218.225.68] Invalid URI in request GET /DomainFiles/*//../../../../../../../../../../etc/passwd H
TTP/1.1
[Wed Jun 20 09:17:32 2018] [error] [client 91.218.225.68] Invalid URI in request GET /../../../../../../../../../../etc/passwd HTTP/1.1
[Wed Jun 20 09:18:00 2018] [error] [client 91.218.225.68] Invalid URI in request GET /file/../../../../../../../../../etc/ HTTP/1.1
[Wed Jun 20 09:18:24 2018] [error] [client 91.218.225.68] Invalid URI in request GET ../../../../../../../../../../etc/* HTTP/1.1
[Wed Jun 20 09:18:24 2018] [error] [client 91.218.225.68] Invalid URI in request GET ../../../../../../../../../../etc/passw* HTTP/1.1
[Wed Jun 20 09:24:03 2018] [error] [client 91.218.225.68] Invalid URI in request GET /../../windows/dvr2.ini HTTP/1.1
[Wed Jun 20 09:24:03 2018] [error] [client 91.218.225.68] Invalid URI in request GET /htdocs/../../../../../../../../../../../etc/passwd HTTP/1
.1
[Wed Jun 20 09:24:05 2018] [error] [client 91.218.225.68] Invalid URI in request GET /help/../../../../../../../../../../../../../../../../../etc/
shadow HTTP/1.1
student@attackdefense:~$
```

But this grep expression may not cover all, so we can use

Command: grep "Invalid URI" error.log

```
student@attackdefense:~$  grep "Invalid URI" error.log
[Wed Jun 20 09:17:28 2018] [error] [client 91.218.225.68] Invalid URI in request GET /../../../../../../../../../boot.ini HTTP/1.1
[Wed Jun 20 09:17:28 2018] [error] [client 91.218.225.68] Invalid URI in request GET /../../../../winnt/repair/sam._ HTTP/1.1
[Wed Jun 20 09:17:29 2018] [error] [client 91.218.225.68] Invalid URI in request GET /DomainFiles/*//../../../../../../../../../../etc/passwd H
TTP/1.1
[Wed Jun 20 09:17:32 2018] [error] [client 91.218.225.68] Invalid URI in request GET /../../../../../../../../../../etc/passwd HTTP/1.1
[Wed Jun 20 09:17:32 2018] [error] [client 91.218.225.68] Invalid URI in request GET /%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/windows/win.ini HTTP/1
.1
[Wed Jun 20 09:17:32 2018] [error] [client 91.218.225.68] Invalid URI in request GET /%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/pass
wd HTTP/1.1
[Wed Jun 20 09:18:00 2018] [error] [client 91.218.225.68] Invalid URI in request GET /file/../../../../../../../../../etc/ HTTP/1.1
[Wed Jun 20 09:18:17 2018] [error] [client 91.218.225.68] Invalid URI in request GET /../webserver.ini HTTP/1.1
[Wed Jun 20 09:18:24 2018] [error] [client 91.218.225.68] Invalid URI in request GET ../../../../../../../../../../etc/* HTTP/1.1
[Wed Jun 20 09:18:24 2018] [error] [client 91.218.225.68] Invalid URI in request GET ../../../../../../../../../../etc/passw* HTTP/1.1
[Wed Jun 20 09:18:25 2018] [error] [client 91.218.225.68] Invalid URI in request GET /../config.dat HTTP/1.1
[Wed Jun 20 09:23:53 2018] [error] [client 91.218.225.68] Invalid URI in request GET /sdk/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/etc/vmware/
hostd/vmInventory.xml HTTP/1.1
[Wed Jun 20 09:24:03 2018] [error] [client 91.218.225.68] Invalid URI in request GET /../../windows/dvr2.ini HTTP/1.1
[Wed Jun 20 09:24:03 2018] [error] [client 91.218.225.68] Invalid URI in request GET /htdocs/../../../../../../../../../../../etc/passwd HTTP/1
.1
[Wed Jun 20 09:24:05 2018] [error] [client 91.218.225.68] Invalid URI in request GET /help/../../../../../../../../../../../../../../../../../etc/
shadow HTTP/1.1
student@attackdefense:~$
```

And the total count will be 15

Command: grep "Invalid URI" error.log | wc -l

Question 5: How many URLs were requested in path bruteforcing attack?

Answer: 229112

Solution:

Command: grep "File does not exist" error.log | wc -l

```
student@attackdefense:~$ grep "File does not exist" error.log  | wc -l
229112
student@attackdefense:~$
student@attackdefense:~$
student@attackdefense:~$ grep "File does not exist" error.log  | head -10
[Sat Dec 12 19:02:36 2015] [error] [client 191.182.199.16] File does not exist: /var/www/www.almhuette-raith.at/templates/_system/css/general.c
ss
[Sat Dec 12 19:44:06 2015] [error] [client 188.45.108.168] File does not exist: /var/www/www.almhuette-raith.at/templates/_system/css/general.c
ss
[Sat Dec 12 19:44:15 2015] [error] [client 188.45.108.168] File does not exist: /var/www/www.almhuette-raith.at/favicon.ico
[Sun Dec 13 01:01:19 2015] [error] [client 157.55.39.3] File does not exist: /var/www/www.almhuette-raith.at/icons/text.gif
[Sun Dec 13 11:28:41 2015] [error] [client 212.95.7.131] File does not exist: /var/www/www.almhuette-raith.at/templates/_system/css/general.css
[Sun Dec 13 12:05:25 2015] [error] [client 40.77.167.66] File does not exist: /var/www/www.almhuette-raith.at/apache-log/error.log.44.gz
[Sun Dec 13 15:56:36 2015] [error] [client 185.104.219.254] File does not exist: /var/www/www.almhuette-raith.at/apache-log/access.log.69.gz
[Sun Dec 13 16:14:58 2015] [error] [client 157.55.39.8] File does not exist: /var/www/www.almhuette-raith.at/apache-log/error.log.55.gz
[Sun Dec 13 18:29:14 2015] [error] [client 188.23.50.138] File does not exist: /var/www/www.almhuette-raith.at/templates/_system/css/general.cs
s
[Sun Dec 13 18:29:18 2015] [error] [client 188.23.50.138] File does not exist: /var/www/www.almhuette-raith.at/favicon.ico
student@attackdefense:~$
```

Question 6: Create a list of all unique URLs used during the path bruteforcing.

Solution:

Command: grep "File does not exist" error.log | cut -d "]" -f4 | cut -d ":" -f2 | sort | uniq > list

```
student@attackdefense:~$ grep "File does not exist" error.log  | cut -d "]" -f4 | cut -d ":" -f2 | sort | uniq > list
student@attackdefense:~$
student@attackdefense:~$ cat list | head -10
 /bin/public_html
 /home/ftp/public_html/
 /nonexistent/public_html/etc/passwd
 /root/public_html/
 /var/www/www.almhuette-raith.at/
 /var/www/www.almhuette-raith.at/  .php
 /var/www/www.almhuette-raith.at/  /
 /var/www/www.almhuette-raith.at/ -
 /var/www/www.almhuette-raith.at/ -.php
 /var/www/www.almhuette-raith.at/ -/
student@attackdefense:~$
```

Question 7: Print the super-set of all types of errors present in the log file?

Answer:

- user X not found
- no acceptable variant
- script not found or unable to stat
- Invalid URI in request
- client denied by server configuration
- File does not exist
- Invalid Content-Length

Solution:

The following command can be used to sort and remove duplicates upto some extent. But, then either you have to check the different logs manually or using other commands.

Command: cat error.log | cut -d "]" -f4 | cut -d ":" -f1 | sort | uniq

```
student@attackdefense:~$ cat error.log | cut -d "]" -f4 | cut -d ":" -f1 | sort | uniq

 File does not exist
 Invalid Content-Length
 Invalid URI in request GET ../../../../../../../../../../etc/* HTTP/1.1
 Invalid URI in request GET ../../../../../../../../../../etc/passw* HTTP/1.1
 Invalid URI in request GET /%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/windows/win.ini HTTP/1.1
 Invalid URI in request GET /%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd HTTP/1.1
 Invalid URI in request GET /../../../../../../../../../../etc/passwd HTTP/1.1
 Invalid URI in request GET /../../../../../../../../../../boot.ini HTTP/1.1
 Invalid URI in request GET /../../../../winnt/repair/sam._ HTTP/1.1
 Invalid URI in request GET /../../windows/dvr2.ini HTTP/1.1
 Invalid URI in request GET /../config.dat HTTP/1.1
```