http://articles.slicehost.com/2010/8/27/reading-apache-web-logs

Combined log components

The first entry is the IP address of the web client accessing your server.

The second entry above is "-", which is what gets logged when there's nothing to put in that part of the log. In this case, the entry would represent the name of a remote log, if one were being used. You'll pretty much always see "-" here.

The third entry above is another "-". That slot contains the username the web client was authorized under, if any. If you enabled password protection for a file or directory, then the username the visitor used to log in would be recorded here.

The next entry is the date and time of the access.

The next entry is the first line of the request the web client sent to the server. In this case it's:

```
POST /wordpress3/wp-admin/admin-ajax.php HTTP/1.1
```

That entry means the web client sent a "POST" request (a submission of information) to the file at "/wordpress3/wp-admin/admin-ajax.php". That's a relative location, which means that if you wanted to find that file you'd start at the document root of that virtual host. If your document root was "/var/www", then the file being accessed above would be at "/var/www/wordpress3/wp-admin/admin-ajax.php". The last entry describes the protocol used for the request, in this case HTTP version 1.1.

The next entry tells us the status code that was returned for the request. The code above, "200", is hopefully one you'll see most often in your access logs — it means that the file was found and served to the client. Other common status codes are "403" (access forbidden) and "404" (file not found). We go into more detail about status codes in **another article**, but for a full list you can visit the official **w3 website's list** of status codes.

The next number is the size of the response your server sent, in bytes. In this case it was a very small response (2 bytes), so it was likely just an acknowledgement from the server rather than a full page access.

The next entry is the "referrer URL". In this case the entry is:

```
http://www.example.com/wordpress3/wp-admin/post-new.php
```

That's the page the web client visited before sending the recorded access request. Usually that means it's the page that linked to the one they accessed. The referrer can be useful information if you're wondering where people are finding links to your site (from a Google search, or a link from a partner site), or if you want to find the page that contained a bad link if the access entry was an error.

The last entry is called the "user agent". Most of the time that just means it's the identifier used by the web browser the visitor used. In this case, the user agent was:

```
Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_4; en-US)
AppleWebKit/534.3 (KHTML, like Gecko) Chrome/6.0.472.25
Safari/534.3
```

The user agent is pretty specific sometimes. In this entry the web browser told the server not only what its name was (Chrome, in this case), but also what operating system it's running on (Mac OS X), the version of the browser and the system, and the components that the web browser uses from the operating system. It's usually a lot more than you need, but if you know your site will display differently in different browsers, all that information can be used by a web application to tailor the page it returns to look best on that particular visitor's browser.

Putting them together

Whew! Lots of stuff there, but it's useful stuff. To give another example, let's look in again on our would-be intruder from earlier. Looking in the error log I saw what time he tried to access the non-existent directory. By looking at the same time in the access log I can see more information about what he tried to access:

```
80.154.42.54 - - [23/Aug/2010:15:25:35 +0000] "GET /phpmy-
admin/scripts/setup.php HTTP/1.1" 404 347 "-" "ZmEu"
```

There's the same IP address and the same time. So we can see that his script used a "GET" method (a request for a page) to ask for the setup script for php-myadmin. The "404" status means that the file wasn't found. And while the user agent entry certainly isn't any web browser on the market, some web searches will turn up other people who have been hit by what is probably the same script. So even if that user agent isn't the browser, it can be useful in determining the type of attack your site was experiencing, and how many 404s you can expect your server to have to handle when it hits you.

access_log

1. What type of log files are they?

   These are GET requests (Request Type, Document URI, and Protocol.)

2. What are the dates which are represented by the logs?

   December 8 – 10, 2013

3. How many unique users appear?
   over 100 different users

4. What was the largest data export? and does it look out of the ordinary? The largest file was 87498 bytes and was an image request

5. What is the most common error found in the error logs?

   Baiduspider/2.0; +http://www.baidu.com/search/spider.html

6. Do you see anything which is out of the ordinary?

   The POST requests look different than the others with a lot of % signs which I think are spaces. I went to http://meyerweb.com/eric/tools/dencoder/ and decoded them.

7. Write a short synopsis of what you found.

   The are a lot of requests from http://clinical-security.com which tells me someone is troubleshooting.

This log format is in the “CLF” combined log format.

A lot of the logs are 200 which means the file was found and served to the client. I found a 404 which means the file was not found. I found a 403 which access was forbidden but right after that they were given access.

access_log-20131117

1. What type of log files are they?
   These are GET requests

2. What are the dates which are represented by the logs?
   10/Nov/2013:03:49:36 to 17/Nov/2013:03:00:01

3. How many unique users appear?
   over 100 different users

4. What was the largest data export? and does it look out of the ordinary?
   over 31,000 and was from http://clinical-security.info

5. What is the most common error found in the error logs?
   I did not see an “error” but saw a ton of 200

   A lot of 403’s http://clinical-security.com

6. Do you see anything which is out of the ordinary? Did not

Write a short synopsis of what you found.

access_log-20131124

7. What type of log files are they?
   These are GET requests

8. What are the dates which are represented by the logs?
   17/Nov/2013:03:17:20 to 24/Nov/2013:03:19:12

9. How many unique users appear?
   over 100 different users

10. What was the largest data export? and does it look out of the ordinary?
    over 31,000 and was from http://clinical-security.info looking for jquery

11. What is the most common error found in the error logs?
    I did not see an “error” but saw a ton of 200

    A lot of 403’s http://clinical-security.com

12. Do you see anything which is out of the ordinary? Did not

Write a short synopsis of what you found.
89.107.227.52 had a lot of 404 errors with w00tw00t.at.blackhats.romanian.anti-sec
It appears that your server is the target of an automated attack involving the ZmEu scanner. That first request appears to be from another automated attack involving the Morfeus Scanner.

That last request appears to be an attempt to exploit vulnerabilities in the Home Network Administration Protocol (HNAP) implementations of D-Link routers

access_log-20131201

13. What type of log files are they?
These are GET requests but several POST from 193.34.205.54. Had to decode them to see the 404 message

14. What are the dates which are represented by the logs?
24/Nov/2013:03:47:21 to 01/Dec/2013:03:00:02

15. How many unique users appear?
over 100 different users

16. What was the largest data export? and does it look out of the ordinary?
over 31,000 and was from http://clinical-security.info looking for jquery

17. What is the most common error found in the error logs?
I did not see an "error" but saw a ton of 200

A lot of 403's http://clinical-security.com

18. Do you see anything which is out of the ordinary?

193.239.186.158 - - [28/Nov/2013:08:34:48 +0000] "GET /user/soapCaller.bs HTTP/1.1" 404 296 "-" "Morfeus Fucking Scanner"
It's a replacement text editor for web sites along the lines of TinyMCE. If you do not have that code installed on your web site then you can ignore those probes. Their looking to exploit a code weakness on your system and those URL requests happen all the time.

CFIDE/administrator/enter.cfm allows one to log into the CF8 admin area

"Baiduspider" is the official name of Baidu's web crawling spider. It crawls web pages and returns updates to the Baidu index.

Top 10 good BOTS

Googlebot
Baidu Spider
MSN Bot/BingBot
Yandex Bot
Soso Spider
ExaBot
Sogou Spider
Google Plus Share
Facebook External Hit
Google Feedfetcher

access_log-20131208

19. What type of log files are they?
    These are GET requests but several POST from 193.34.205.54. Had to decode them to see the 404 message

20. What are the dates which are represented by the logs?
    01/Dec/2013:03:33:45 to 08/Dec/2013:03:14:58

21. How many unique users appear?
    over 100 different users

22. What was the largest data export? and does it look out of the ordinary?
    over 31,000 and was from http://clinical-security.info looking for jquery

23. What is the most common error found in the error logs?
    I did not see an “error” but saw a ton of 200

    A lot of 403’s http://clinical-security.com

24. Do you see anything which is out of the ordinary?

124.32.177.202 - - [07/Dec/2013:14:44:28 +0000] "HEAD http://209.20.69.216:80/mysql/admin/ HTTP/1.1" 404 - "-" "revolt"---- this showed up many times

198.27.67.38 - - [05/Dec/2013:15:48:47 +0000] "GET /?q=node/30++Result:+no+post+sending+forms+are+found; HTTP/1.0" 404 5342 "http://clinical-security.com/?q=node/30++Result:+no+post+sending+forms+are+found;" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1.0 Safari/537.11"
"no post sending forms" doesn't necessarily mean there's an error with xrumer. Most of the time it means that the URL either is 1) down or 2) no longer a forum and xrumer simply cannot find any of the standard fields it uses to register.

aiHitBot
aiHit is a leading Business to Business provider of business information services and solutions.

error_log

25. What type of log files are they?
    error logs

26. What are the dates which are represented by the logs?
    Dec 08 03:38:07 2013 to Tue Dec 10 18:42:06 2013

27. How many unique users appear?
    15

28. What was the largest data export? and does it look out of the ordinary?

29. What is the most common error found in the error logs?
    script not found or unable to stat: /var/www/cgi-bin/php
    File does not exist

30. Do you see anything which is out of the ordinary?
Digest: generating secret for digest authentication ...

error_log-20131117

31. What type of log files are they?
error logs

32. What are the dates which are represented by the logs?
Sun Nov 10 03:38:07 2013 to Sun Nov 17 03:14:06 2013

33. How many unique users appear?
22

34. What was the largest data export? and does it look out of the ordinary?

35. What is the most common error found in the error logs?
File does not exist

36. Do you see anything which is out of the ordinary?

/var/www/html/w00tw00t.at.blackhats.romanian.anti-sec:)

error_log-20131124

37. What type of log files are they?
error logs

38. What are the dates which are represented by the logs?
Sun Nov 17 03:14:07 2013 to Sun Nov 24 03:36:14 2013

39. How many unique users appear?
17

40. What was the largest data export? and does it look out of the ordinary?

41. What is the most common error found in the error logs?
script not found or unable to stat: /var/www/cgi-bin/php
File does not exist

Do you see anything which is out of the ordinary?
Backtrace

Memory Map

/lib64/libnss_files-2.12.so
too lazy to change the Makefiles to allow the generation of shared objects not starting with `lib`

error_log-20131201

42. What type of log files are they?
error logs

43. What are the dates which are represented by the logs?

Sun Nov 24 03:36:15 2013 to Sun Dec 01 03:29:13 2013

44. How many unique users appear?
31

45. What was the largest data export? and does it look out of the ordinary?

46. What is the most common error found in the error logs?
script not found or unable to stat: /var/www/cgi-bin/php
File does not exist

Do you see anything which is out of the ordinary?

[warn] child process 316 still did not exit, sending a SIGTERM

means

cPanel will automatically try to restart Apache

error_log-20131201 (1)

What type of log files are they?
error logs

47. What are the dates which are represented by the logs?
Sun Nov 24 03:36:15 2013 to Sun Dec 01 03:29:13 2013

48. How many unique users appear?
27

49. What was the largest data export? and does it look out of the ordinary?

50. What is the most common error found in the error logs?
script not found or unable to stat: /var/www/cgi-bin/php
File does not exist

Do you see anything which is out of the ordinary?

File does not exist: /var/www/html/FCKeditor

child process 316 still did not exit, sending a SIGTERM
Apache Failing

error_log-20131208

What type of log files are they?
error logs

51. What are the dates which are represented by the logs?
Sun Dec 01 03:29:14 2013 to Sun Dec 08 03:38:06 2013

52. How many unique users appear?
27

53. What was the largest data export? and does it look out of the ordinary?

54. What is the most common error found in the error logs?
script not found or unable to stat: /var/www/cgi-bin/php
File does not exist

Do you see anything which is out of the ordinary?

Invalid URI in request GET HTTP/1.1 HTTP/1.1

Messages

What type of log files are they?
messages

55. What are the dates which are represented by the logs?
Dec 8 03:38:03 to Dec 10 20:45:39

56. How many unique users appear?

57. What was the largest data export? and does it look out of the ordinary?

58. What is the most common error found in the error logs?
clinical-security-lamp kernel

It means you haven't registered the system into RHN

59. Do you see anything which is out of the ordinary?

auditd[901]: Audit daemon rotating log files
clinical-security-lamp rhsmd: This system is registered to RHN Classic

Secure

What type of log files are they?
messages

60. What are the dates which are represented by the logs?
Dec 8 03:56:07 to Dec 10 20:28:19

61. How many unique users appear?

62. What was the largest data export? and does it look out of the ordinary?

63. What is the most common error found in the error logs?
authentication failure

64. Do you see anything which is out of the ordinary?

failed - POSSIBLE BREAK-IN ATTEMPT!

Normal Shutdown, Thank you for playing

pam_unix(sshd:auth): authentication failure

The pam_unix module logs this. See modules/pam_unix/support.c in the pam library sources.