Harmony Betancourt

SID: 0003948694

Log Analysis

Access\_log

**Type**: Access of site  
**Date Range:** Dec 8th, 2013 – Dec 10th, 2013

**Unique Users**: 192

**Largest Data Export:** 87498 from IP 66.249.76.146 on 09/Dec/2013:16:48:26  
 Suspicious: No - Google Bot

**Common Error**: N/A

**Suspicious Activity:** IP address 109.163.229.59 attempted to access the site on 10/Dec/2013:12:04:25, and alter the php configuration, invoking several 404 errors, which may be an indicator of a user unfamiliar with the file structure. When paired with the user’s seeming unfamiliarity with the version of php being used, research further to fully assess risk and if it is the IP address of an administrator.

**Synopsis**: This access log files has tracked the requests of every IP on the site between Dec 8th and Dec 10th of 2013. There were 192 unique users accessing the site through that time period, with the largest request from a googlebot for an image. There was suspicious activity on December 10th, 2013 involving requests to post changes to the php configuration.

Access\_log-20131117

**Type:** Access of site  
**Date Range:** Nov 10th, 2013 – Nov 17th, 2013

**Unique Users:** 414

**Largest Data Export:** 67968 **Suspicious:** No – PNG image

**Common Error:** N/A

**Suspicious Activity:** On the dates within the log file, there may have been an attack on the site. IP Addresses 80.72.38.195, 80.72.37.190, 80.72.37.187, 80.72.37.178, 80.72.36.202, 80.72.35.91, 80.72.35.87, 80.72.35.86, 79.141.167.28, 79.133.217.242, 79.133.216.99, 79.133.200.59, 79.133.200.202, and 79.133.196.50, attempted to register and add users to the database at a repeated speed that seems unlikely for a human making errors, and at the same time. Further research indicated that all of these addresses have been reported as spammers across multiple boards and reporting agencies.

**Synopsis:** This access log files has tracked the requests of every IP on the site between Nov 10th and Nov 17th of 2013. There were 414 unique users accessing the site through that time period, with the largest request for an image. There was suspicious activity throughout the log involving multiple requests from IP addresses similar enough to warrant concern, enacting requests at a rapid rate at the same time, which may be an attack on the system.

Access\_log-20131124

**Type:** Access of site  
**Date Range:** Nov 17th 2013 – Nov 24th 2013

**Unique Users:** 393

**Largest Data Export:** 45611 **Suspicious:** No – Image request

**Common Error:** N/A

**Suspicious Activity:** On Nov 22 between 20:56:20 and 20:56:23 IP address 211.240.5.133 attempted to alter the php configuration, invoking several 404 errors, which may be an indicator of a user unfamiliar with the file structure. When paired with the user’s seeming unfamiliarity with the version of php being used, research further to fully assess risk and if it is the IP address of an administrator.

On Nov 18th between 15:22:06 IP 109.252.230.134 Attempted to access the site using GET /w00tw00t.at.blackhats.romanian.anti-sec:) HTTP/1.1, then access phpMyAdmin as well as the php setup.This happened again on Nov 19th between 15:01:48 and 15:05:30 by IP address 89.107.227.52, the 21st of November at 16:11:47 from IP address 63.141.227.74, on Nov 21st at 17:0508 from IP address 208.109.209.94, and November 22nd at 15:19:05 from IP 46.246.124.16.

On Nov 20th from 22:53:14 – 22:54:42 IP address 46.137.84.101 attempted to access the site using GET /muieblackcat HTTP/1.1 before attempting to access and change phpMyAdmin, MySQL, and the php configuration, invoking 404 errors the entire time.

**Synopsis:** This access log files has tracked the requests of every IP on the site between Nov 17th and Nov 24th of 2013. There were 393 unique users accessing the site through that time period, with the largest request for an image. There was suspicious activity throughout the log involving multiple requests from IP addresses with an alarming GET request that utilizes slang for hacking, as well as attempts to change the configuration of the site.

Access\_log-20131201

**Type:** Access of site  
**Date Range:** Nov 24th 2013 – Dec 1st 2013

**Unique Users:** 398

**Largest Data Export:** 75411 **Suspicious:** No – PNG image

**Common Error:** N/A

**Suspicious Activity:** IP address 193.34.205.54 attempted to access the site on 24/Nov/2013, and alter the php configuration, invoking several 404 errors, which may be an indicator of a user unfamiliar with the file structure. This occurred again from IP 188.138.90.43 on the 29th of Nov between 15:12:00 and 15:12:01, and from IP 192.34.63.145 between 17:24:12 and 17:24:13

On Nov 24thth between 12:05:08 and 12:05:11 IP 154.44.190.122 attempted to access the site using GET /w00tw00t.at.blackhats.romanian.anti-sec:) HTTP/1.1, then access phpMyAdmin as well as the php setup.

**Synopsis:** This access log files has tracked the requests of every IP on the site between Nov 24th and Dec 1st of 2013. There were 398 unique users accessing the site through that time period, with the largest request for an image. There was suspicious activity throughout the log involving multiple requests from IP addresses with an alarming GET request that utilizes slang for hacking, as well as attempts to change the configuration of the site.

Access\_log-20131208

**Type:** Access of site  
**Date Range:** Dec 1st 2013 – Dec 8th 2013

**Unique Users:** 382

**Largest Data Export:** 97598 **Suspicious:** No – Image – May want to compress more

**Common Error:** N/A

**Suspicious Activity:**  On Dec 2nd between 13:18:13 and 13:18:14 IP 89.248.160.192 attempted to access the site using GET /w00tw00t.at.blackhats.romanian.anti-sec:) HTTP/1.1, then access phpMyAdmin as well as the php setup. This occurred again, from IP 211.89.225.234 on Dec 2nd from 01:41:31 to 01:41:33, on Dec 7th from 6:20:59 - 6:21:03 by IP 89.248.171.50 and from 16:20:27 to 16:20:29 by IP 119.254.230.171.

On Dec 4th from 01:02:27 to 01:02:28 IP address 87.106.244.93 attempted to access the site using GET /muieblackcat HTTP/1.1 before attempting to access and change phpMyAdmin, MySQL, and the php configuration, invoking 404 errors the entire time.

IP address 208.71.112.190 attempted to access the site on Dec 5th at 07:06:21 and alter the php configuration, invoking several 404 errors, a reattempt from the same IP occurred at 07:20:19, and again from IP 41.57.104.190 on Dec 6th between 05:47:55 and 05:48:09, and Dec 8th between0 9:02:05 and 09:02:07 by IP 195.244.39.213

On Dec 7th, what appears to be an attempt to access information on the database and structure of the website as well as administration information from IP address 124.32.177.202 between the times of 02:53:56 and 2:54:29, with 97 HEAD requests made during that time frame. This happened again on the same day between 14:44:28 and 14:45:01

**Synopsis:** This access log files has tracked the requests of every IP on the site between Dec 1st and Dec 8th of 2013. There were 382 unique users accessing the site through that time period, with the largest request for an image. There was suspicious activity throughout the log involving multiple requests from IP addresses with an alarming GET request that utilizes slang for hacking, as well as attempts to change the configuration of the site, and what appears to be an attempt to access information about the database and administration of the site.

Error\_log

**Type:** Error Log  
**Date Range:** Dec 8th – Dec 10th 2013

**Unique Users:** 18

**Largest Data Export:** N/A **Suspicious:** N/A

**Common Error:** Script Not Found or unable to stat, file not found

**Suspicious Activity:** Possible **Synopsis:** This error log covers the dates of December 8th through December 10th, with the most common errors being those of files or scripts being nonexistent, or unable to be accessed due to security controls.In and of themselves, these errors can be indicative of an attempt to find files that are not on the server, but in conjunction with the activity on the log, these errors should be looked into further to assess a security risk.

Error\_log-20131117

**Type:** Error Log  
**Date Range:** Nov 10th – Nov 17th 2013

**Unique Users:** 26

**Largest Data Export:** N/A **Suspicious:** N/A

**Common Error:** File Not Found

**Suspicious Activity:** Possible **Synopsis:** This error log covers the dates of November 10th through November 17th 2013 with the most common error being file not found.In and of itself, this error can be indicative of an attempt to find files that are not on the server and is common, but in conjunction with the activity on the log, these errors should be looked into further to assess a security risk.

Error\_log-20131124

**Type:** Error Log  
**Date Range:** Nov 17th – Nov 24th 2013

**Unique Users:** 31

**Largest Data Export:** N/A **Suspicious:** N/A

**Common Error:** File Not Found

**Suspicious Activity:** Yes **Synopsis:** This error log covers the dates of November 17th through November 24th 2013 with the most common error being file not found.In and of itself, this error can be indicative of an attempt to find files that are not on the server and is common, but in conjunction with the activity log and the sheer number of errors in such rapid succession, as well as the activation of the back trace upon a fatal error are indicative of a possible attack on the site.

Error\_log-20131201

**Type:** Error Log  
**Date Range:** Nov 24th – Dec 1st

**Unique Users:** 34

**Largest Data Export:** N/A **Suspicious:** N/A

**Common Error:** File Not Found

**Suspicious Activity:** Yes **Synopsis:** This error log covers the dates of November 24th through December 1st 2013 with the most common error being file not found.In and of itself, this error can be indicative of an attempt to find files that are not on the server and is common, but in conjunction with the activity log and the sheer number of errors in such rapid succession from the same IP addresses, this is highly suspicious and should be investigated further.

Error\_log-20131208

**Type:** Error Log  
**Date Range:** Dec 1st – Dec 7th 2013

**Unique Users:** 27

**Largest Data Export:** N/A **Suspicious:** N/A

**Common Error:** File Not Found

**Suspicious Activity:** Yes **Synopsis:** This error log covers the dates of December 1st through December 7th 2013 with the most common error being file not found.In and of itself, this error can be indicative of an attempt to find files that are not on the server and is common, but in conjunction with the activity log and the sheer number of errors in such rapid succession from the same IP addresses, this is highly suspicious and should be investigated further.

Messages

**Type:** Message Log  
**Date Range:** Dec 8 - Dec 13 2013

**Unique Users:** 239

**Largest Data Export:  
 Suspicious:**

**Common Error:**

**Suspicious Activity:  
Synopsis:** This message log has the source IP, destination IP, and information about the user’s computer.

Secure

**Type:** Secure Log  
**Date Range:** Dec 8th – Dec 10th 2013

**Unique Users:** 15 (Including root)

**Largest Data Export:  
 Suspicious:**

**Common Error:**

**Suspicious Activity:** YES  **Synopsis:** This security log notes all the failed attempts to access secure areas of the site, as well as how many attempts were made, and why the attempts were unsuccessful. According to this report there may have been at least 13 attempts from non-authorized users to access secure information. This report must absolutely be followed up to ensure security is not breached and any weaknesses are repaired.