­­Cory Wilson

NSS1501

Log Analysis

File: access\_log

1. What type of log files are they?
   * Access Logs
2. What are the dates that are represented by the logs?
   * December 8-10, 2013
3. How many unique users appear?
   * 577
4. What was the largest data export? And does it look out of the ordinary?
   * IP: 66.249.76.134
   * 87498
5. What is the most common error found in the error logs?
   * 200 Error
6. Write a short synopsis of what you found.
   * This shows the log files for http access attempts from December 8-10, 2013.

File: access\_log-20131117

1. What type of log files are they?
   * Access Logs
2. What are the dates that are represented by the logs?
   * November 10-17, 2013
3. How many unique users appear?
   * 1752
4. What was the largest data export? And does it look out of the ordinary?
   * IP: 199.30.20.84
   * 67968
5. What is the most common error found in the error logs?
   * 200 Error
6. Do you see anything out of the ordinary?
   * Some Romanian sites accessed the page
7. Write a short synopsis of what you found.
   * This shows the log files for http access attempts on 11/17/2013.

File: access\_log-20131124

1. What type of log files are they?
   * Access Logs
2. What are the dates that are represented by the logs?
   * November 17 -24, 2013
3. How many unique users appear?
   * 1979
4. What was the largest data export? And does it look out of the ordinary?
   * IP: 146.120.158.93
5. What is the most common error found in the error logs?
   * 200 Error
6. Write a short synopsis of what you found.
   * These are the http access logs for November 17-24, 2013.

File: access\_log-20131201

1. What type of log files are they?
   * Access Logs
2. What are the dates that are represented by the logs?
   * November 24 – December 1, 2013
3. How many unique users appear?
   * 1807
4. What was the largest data export? And does it look out of the ordinary?
   * IP: 61.135.190.222
   * 31028
5. What is the most common error found in the error logs?
   * 200 Error
6. Write a short synopsis of what you found.
   * These are the http access logs from November 24, 2013 – December 1, 2013.

File: access\_log-20131208

1. What type of log files are they?
   * Access Logs
2. What are the dates that are represented by the logs?
   * December 1 – 7, 2014
3. How many unique users appear?
   * 1854
4. What was the largest data export? And does it look out of the ordinary?
   * IP: 209.242.132.126
   * 10959
5. What is the most common error found in the error logs?
   * 200 Error
6. Do you see anything out of the ordinary?
   * An access attempt from http://pspstrana.ru/
7. Write a short synopsis of what you found.
   * These are the http access logs from December 1 – 7, 2014.

File: error\_log

1. What type of log files are they?
   * Error Logs
2. What are the dates that are represented by the logs?
   * December 8 – 10, 2013
3. How many unique users appear?
   * 19
4. What is the most common error found in the error logs?
   * File Does Not Exist
5. Do you see anything out of the ordinary?
   * No
6. Write a short synopsis of what you found.
   * In these error logs the most common error was a file does not exist. So I would assume the user was looking for a page that simply didn’t exist. Other common errors were script not found.

File: error\_log-20131117

1. What type of log files are they?
   * Error Logs
2. What are the dates that are represented by the logs?
   * November 10 – 17, 2013
3. How many unique users appear?
   * 30
4. What is the most common error found in the error logs?
   * File Does Not Exist
5. Do you see anything out of the ordinary?
   * A notice about Apache being configured.
6. Write a short synopsis of what you found.
   * The most common error logged here was a file does not exist. Second most common was script not found.

File: error\_log-20131124

1. What type of log files are they?
   * Error Logs
2. What are the dates that are represented by the logs?
   * November 17 – 24, 2013
3. How many unique users appear?
   * 57
4. What is the most common error found in the error logs?
   * Child process “X” does still did not exit.
5. Do you see anything out of the ordinary?
   * Not sure what child process did not exit means. It’s the first time I’ve come across it.

File: error\_log-20131201

1. What type of log files are they?
   * Error Logs
2. What are the dates that are represented by the logs?
   * November 24 – December 1, 2013
3. How many unique users appear?
   * 51
4. What is the most common error found in the error logs?
   * File Does Not Exist
5. Do you see anything out of the ordinary?
   * Child process still did not exit is still present.

File: error\_log-20131201 (1)

1. What type of log files are they?
   * Error Logs
2. What are the dates that are represented by the logs?
   * November 24 – December 1, 2013
3. How many unique users appear?
   * 51
4. What is the most common error found in the error logs?
   * File Does Not Exist
5. Do you see anything out of the ordinary?
   * Child process still did not exit.

File: error\_log-20131208

1. What type of log files are they?
   * Error Logs
2. What are the dates that are represented by the logs?
   * December 1 – December 8, 2013
3. How many unique users appear?
   * 31
4. What is the most common error found in the error logs?
   * File Does Not Exist

File: messages

1. What type of log files are they?
   * Message Logs
2. What are the dates that are represented by the logs?
   * December 8 – 10, 2013
3. How many unique users appear?
   * 501

File: secure

1. What type of log files are they?
   * Secure Logs
2. What are the dates that are represented by the logs?
   * December 8 – 10, 2013
3. How many unique users appear?
   * 7300