NSS1405_Beyer_Matthew

What type of log file is it?

The log files consist of 5 Access logs and 6 Error logs (one is a duplicate so 5) , a Auth log and a Server Message log.

What are the dates which are represented by the logs?

The dates range from November 10th 2013 to December 10th 2013.

How many unique users appear?

I could go through all the of these and get the exact number but that would not be very practical. The access log should have a summary report available, which is what I would use if I really wanted to know.

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

The largest data export is — GET /sites/default/files/images/Daly.png HTTP/1.1 (at 97598b) it is an image and it does not seem to out of the ordinary.

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

Error 403 Forbidden.

Do you see anything which is out of the ordinary?

A few things seem out of the ordinary, mostly from w00tw00t.at.blackhats.romanian.anti-sec:) HTTP/1.1

Write a short synopsis of what you found in each file.

The majority of the access logs are typical behavior, just logs on successful posts with a few failures sprinkled in - nothing really unusual to report there, or not that I can make out. The part that stands out immediately are on the error logs, where (w00tw00t.at.blackhats.romanian.anti-sec:) HTTP/1.1) is repeatedly trying to access the server config files from varying IP's. The auth log also has some suspicious activity, or really, not-so-suspicious and more blatantly obvious, with someone attempting to just brute-force the root password, starting on Dec 8th and continuing for several days.