Examine each of the logs and answer the following questions:

1. What type of log files are they?

Access Log, Error Log, System Messages, and Secure Log

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

Access\_Log

December 08, 2013 - December 10, 2013

November 10, 2013 - November 17, 2013

November 17, 2013 - November 24, 2013

November 24, 2013 - December 01, 2013

December 01, 2013 - December 08, 2013

Error\_Log

December 08, 2013 - December 10, 2013

November 10, 2013 - November 17, 2013

November 17, 2013 - November 24, 2013

November 24, 2013 - December 01, 2013

December 01, 2013 - December 08, 2013

System Messages

December 08, 2013 - December 10, 2013

Secure Log

December 08, 2013 - December 10, 2013

1. How many unique users appear?

User: tomcat

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

Dec 10 00:44:14 clinical-security-lamp kernel: IN=eth0 OUT= MAC=40:40:7c:01:70:3c:d0:d0:fd:6d:b5:bf:08:00 SRC=67.22.128.170 DST=209.20.69.216 LEN=694 TOS=0x00 PREC=0x00 TTL=51 ID=0 DF PROTO=UDP SPT=5060 DPT=5060 LEN=674

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

File does not exist: /var/www/

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

It took 2 days(Dec 8th - Dec 10th) of non stop user access to finally get access, Looks like the system was being hacked

1. Write a short synopsis of what you found.

I would say the system was either being hacked or the system received a virus.