Case #2: Compromised HDFS Cluster!

You have been called to analyze a compromised Linux Hadoop Cluster. The cluster includes one Name Node (master) and two Data Nodes (Slaves). There is a suspicion that they all have been compromised, but no proof to that.

Deliverables:

1. How the threat actor gained access to the system?
2. What privileges were obtained and how?
3. What modifications were applied to the system?
4. What persistent mechanisms on each compromised system were being used?
5. Could this system be cleaned/recovered?
6. Recommendations

Outcomes:

At the end of this lab, you will have the required skills to deal with a compromised Linux system, were you will be capable of doing:

1. Listing the volumes and mounting a forensic case image
2. Searching through the FHS
3. Search in log files
4. Understanding system services and how they work
5. Use TSK tools to list info of the image and deal with EXT4 fs
6. Use debugfs, EXT4 journal and ext4magic to recover deleted files
7. Generate and filter a super timeline

Note: please use tables and screenshots to represent your results if needed. Like I usually say "**Screenshot or it didn't happen!**".