BLUE 1

| **Good Things:** | **Missing Things:** |
| --- | --- |
| * Told us what they installed on every service (assume 5 minute plan) * Said a problem with a service and what they did to stop it / fix it * Included images * Breakdown of what every member did and what service they were in charge of * Had a good attitude throughout the report | * Didnt really elaborate on the injects, talked about silly day as well as one other inject but not the rest |

BLUE 2

| **Good Things:** | **Missing Things:** |
| --- | --- |
| * Included specific commands that were used during the set up process for both windows and linux * Included a list of IP addresses that were blocked * Did have a breakdown of the injects that they saw | * Two pages of the 5 pages is a list of the commands that they changed * Half a page is a table with their usernames and passwords with no elaboration * The reasons for the blocked IP addresses are pretty much the same * No analysis of anything other than suspicious IPs * No breakdown by person * No “this was a problem and this is how we fixed it” |

In General We Want to See:

* A breakdown of their 5 minute plan
* What each team member did throughout the competition
* Suspicious things they found from what could've been red team
  + What they did to stop it
* The injects that they did

If the total report is worth 50 points:

Blue 1 - 40-45

Blue 2 - 30