TEAM 6: SAXOPHONE GORILLA INTRUSION REPORT (10:00AM)

No intrusion was detected on our servers as of 2016-03-26 9:20AM. Our Nagios Log Server (Centralized Logging) and Nagios XI (Monitoring server) are not throwing any alerts for modification of flag areas, root commands, or config file changes.

Green team user commands are being logged and watched, and so far nothing malicious has been performed on them. Because there were no numerous attempted login attempts, and all the commands have been legitimate within the range of the use of our services, we will still watch these commands, but we do not suspect an intrusion.

No flags have been stolen or planted, as evidenced by the lack of alert of IScore and auditd, which is auditing the directories of red flag locations and files of blue flags.

However, we have had some failed password attempts by some suspicious IP addresses, which we are watching carefully.

Mar 26 08:54:14	192.168.1.99	GitLab	Failed password for root from 12.110.252.211 port 49282 ssh2
Mar 26 08:54:14	192.168.1.99	GitLab	Failed password for root from 12.110.252.211 port 49282 ssh2
Mar 26 08:13:57	192.168.1.77	webserver	Failed password for invalid user shell from 12.110.251.63 port 8460 ssh2
Mar 26 08:10:04	192.168.1.77	webserver	Failed password for cdc from 12.110.251.63 port 8400 ssh2
Mar 26 08:03:42	192.168.1.77	webserver	Failed password for cdc from 148.48.1.123 port 51198 ssh2