Proposed Cyber Operations Contest with Cryptol and SAW

1. There are competing teams plus a competition scorer on a VPN.
2. Each team has a fixed number of members (typically 3) and each member operates a host that is given its own unique IP address on a contest VPN
3. A contest administrator (CA) provides a (compromised) OS for each host and each host must use that OS for the entire contest - the scorer will send a heartbeat request that must be followed by an encrypted reply to check.
4. The hosts are presented to competitors up to a month or two in advance by the contest administrator. This allows competitors to find exploitable vulnerabilities and time to patch them and to develop attacks to be used during the contest.
5. Each host is asked to provide a variety of services: for example some subset of: daytime, echo, chargen, anonymous ftp, time, whois, finger, telnet, mail, web server, mysql, wordpress, cups (and others).
6. Most of the modules for providing these services are custom made, either by the contest administrator or by the developers and exist in a library available to the contest administrator.
7. Each module may have one or more exploitable vulnerabilities.
8. With each module there is a human readable specification that is given to each team member.
9. The human readable specification is the same for every module providing the same service, however OS code will likely be different for each module providing the same service.
10. The scorer is operated by the contest administrator and has two functions. First, it is expected that, prior to the competition, all participants will create a Cryptol spec aligned with each of the provided human readable specifications and those Cryptol specifications will be placed in the ftp directory so that the scorer can transfer the code to itself for testing. The scorer will test the spec against its own known good spec for equivalence. For every service, if equivalence is achieved, then the team member whose host is running that service gets some, initially decided, number of points. Second, every X seconds, where X is determined by the CA, the scorer checks each host for services that are running. Say 1 point is given to a team member for each service that its host is running correctly when the scorer checks.
11. Results are maintained in real time and displayed on a widely accessible web page as a scoreboard, one line for each team member, sorted by decreasing score.
12. It is expected that teams will immediately work on their Cryptol specifications so they can use them with SAW to find vulnerabilities in the supplied service modules.
13. The scoreboard displays ranking by team and by individual
14. At the end of the contest the team with highest points wins.