Red Team: Procedures and Responsibilities

The Red Team represents the “hackers”: malicious users, advanced persistent threats, foreign nation-states, bored kids in a basement, or other agents that may want to cause harm to a Blue Team’s infrastructure. The Red Team is staffed by industry professionals and national laboratory employees and will be chosen by the White Team. The Red Team will evaluate the efforts of the Blue Teams at the completion of the attack phase and provide a score of **0–300 pts**.

Evaluation by Red Team

At the conclusion of the attack phase, the Red Team will evaluate the Blue Teams on the extent to which they have adhered to the spirit of the competition. Teams are scored on the following criteria:

- **0–100 pts:** Did the team take appropriate measures to secure its network that would hold up in a real-world environment, both technically and politically (realistic limits on user accounts, appropriate intervention in user activities, not breaking functionality such as web-based file uploads, etc.)?
- **0–100 pts:** Did the team respond to attacks in a rational and appropriate manner that would be acceptable in a real-world situation, even if simply by having no response (not blocking large ranges of IP addresses, not killing users’ sessions [whack-a-mole], not removing the users’ web content, etc.)?
- **0–100 pts:** This “non-arbitrary” catch-all criterion includes physical security, social engineering, overall conduct (e.g., deduction of points for derogatory “messages” to Red, White, Green, or Blue Teams), or any other noteworthy factors.