



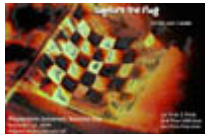
[Welcome](#) | [Capture the Flag](#) | [Student Research Posters](#) | [Cyber Security Quiz](#) | [Digital Forensics Challenge](#) | [Student Essay Contest](#) | [Registration](#)

**Information Systems  
Security Lab**

## Cyber Security Awareness Week [cSAW]

Polytechnic University  
6 MetroTech Center  
Brooklyn, NY 11201

Nov 8 - Nov 10



### Capture the Flag (CTF) Contest

Capture the Flag (CTF) is a team versus team cyber attack and defense competition. CTF functions in the same way as board games such as, King of the Hill and Capture the Flag, in an exciting digital format where only the most skilled teams will succeed. Each team will be delegated a Linux box from which to launch their attacks against a pool of target systems. The overall objective of CTF is to gain control over as many victim computers from the pool and then maintain control of them as long as possible. Prizes totaling \$900 will be given out to the top three teams.

First 15 teams that register to participate will have remote access to the CTF testbed. Competition opens on November 8 and closes on 23:59 EST, 9 November 2004. Winners will be determined by an automated scoring system at the end of the competition. Winners present at the award ceremony on Wednesday, November 10<sup>th</sup> will receive their prizes. Please [register now](#) to assure a place in the CTF. There is no limit on the number of participants in a team.

#### What can I use?

Participants are free to use any tool. To help you get started here is a brief list of [mostly free tools and resources](#).

#### Rules of Engagement

1. Teams are encouraged to bring their own portfolio of tools. All forms of attack are permitted except Denial of Service. Denial of service is expressly forbidden, and if detected, will negatively impact a team's score.
2. Attacks against the scoring server and agents are forbidden and there are protections to prevent such actions. Teams will be penalized for such actions.
3. Teams are connected to the network over a secured channel and will receive their own sandbox within the CTF network. No hardware is required on the part of the teams except for computer access to the network.
4. The objective of the game is for each team to gain root on the target systems and hold them as long as possible during the competition to score points. The scoring system is round-based, thus you must keep your flag for a round to score points.
5. Your flag must be the first discovered, or the only flag in the systems root directory in order to score. Multiple flags can be placed in the root, however only the first one discovered is counted. Locking keys and techniques is permitted and expected. Attackers should know how to clear the other team's flag.
6. Teams can choose to secure the target hosts they gain access to. If a machine is downed it will be taken offline and the current owner will be removed. In this game it's everyman/woman for him/herself. You may hit one another within reason. Subtle and silent wins the race, so don't draw attention to yourself.
7. Keys will be provided to each team, and the key must be planted in the root directory of the target system to get credit for owning it. In the event of more than one flag per server, the first flag planted will get credit. Each team will have the name "team\_", however the agent only cares that the file starts with "team\_". You can rename the rest of the file name anything you want, and can put multiple copies of the flag in the root directory (provided they begin with "team\_" and contain your flag).
8. Teams will lose a fixed amount of points per megabyte of traffic, so use as little traffic as possible. Don't launch DoS, DDoS or massive superscans, you will be penalized.
9. No information will be issued about the network (i.e. OS.s, specific IPs), except for a range of IP addresses.
10. At any time, there may be scheduled "bonus rounds" and "penalty rounds" for gaining bonus points or losing points depending on specific scenarios.
11. The highest total score will determine the winner at the end of the competition. The scoreboard is available on the web browser and can be viewed at anytime by the teams, to check their status. The scoreboard is a summary of how each team is doing, but may not be a reflection of the final results.
12. The Judges can and will modify the behavior of the target hosts at random intervals during the competition. Teams are allowed to probe, analyze, and test the network and all systems attached to it, so plug in at you are. Systems which are down for too long may be rebooted/reimaged by the Judges. The Judges are not responsible for downtime.

- systems connected to the contest network and contestant systems may be subject to remote or Judges and other teams.
13. Social engineering is allowed, however teams shall not be allowed physical access to either target systems. No physical coercion will be tolerated against teams, judges, or bystanders. Either will disqualification.
  14. Teams can and should issue tickets describing their successful attacks through the CTF website that each team receives the points they deserve, if there exist any disputes at the games conclude.
  15. Each team will elect a captain which will be a point of contact for the judges.

**Winners of cSAW 2004 Capture the Flag Contest:**

- **1<sup>st</sup> - Michael Aiello, Polytechnic University Winning Entry**
- **2<sup>nd</sup> - Dan Guido, Eliya Stein, and Darien Acosta, Polytechnic University**
- **3<sup>rd</sup> - Murad Khan, Boris Kochergin, Arlinton Bourne, William Bendick, and "Max", Polytechnic University**

**Photos of the winners:**



**See more photos from the various events...**