悟入戸

CAPTURE THE FLAG WarGamez

What is the goal? To win the game. Teams and individuals so by finding and reporting vulnerabilities (we refer to found vulns as “breakthroughs”), exploiting them on the servers that teams are trying to protect, and ultimately stealing or overwriting teams’ tokens.

Spectator Information

- Each team is assigned a color, reflected on the scoreboard and on their tables. Individual contestants (“ronin”) have a scoreboard color, but they all sit together at the grey table.
- The scoreboard updates every five minutes. There can be a 30 minute lag between when teams submit advisories and when we award breakthrough points.
- We encourage social engineering and other creative ways for teams and individuals to gain an advantage against each other.
- We have an in-game zero-day auction site called eday. Ronin can auction off breakthroughs, or anything else they want. We will occasionally show the eday site on one of the projectors.
- We have some new information visualization techniques which have been released at BlackHat and Defcon that will be highlighted on one of the screens from time to time.
- Contestants are given “totems” that they need to protect, because their entire identity is their totem. Anyone who steals or reproduces the totem effectively becomes the team. Totems are TAB cans with secret information written on the bottom.

GAME BASICS

- Teams defend servers that are running lots of exploitable software.
- Everyone can create accounts, log in and use everyone else’s servers. But only teams have administrative access to their own servers (unless someone exploits the box).
- Kenshoto determines whether services are still running, and docks teams when they can’t keep their services up.
- There are “tokens” on the servers that attackers are trying to steal and/or overwrite. Doing so gives them points.
- Kenshoto changes out tokens from time to time. Teams and individuals can only capture or overwrite a single token once.
- Contestants also score for producing security advisories with working exploit code. Multiple contestants can submit an advisory for the same problem, but the first to do so scores many more points.
- Denial of service is not allowed.
- Rooting a non-team (kenshoto) box via the network is worth massive points. It can be done, it’s just ridiculously hard.
- However... if we catch people trying to hack us before they actually succeed, we will penalize them back into the stone age.
- There will be an individual winner, a team winner and an overall winner. It will be tough, but possible to be a ronin and win the overall game.