悟入戸

CAPTURE THE FLAG WARGAMEZ

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

Ronin Background Information

As a ronin, you will need to find security vulnerabilities, build exploits for them and use them to p0wn tokens that teams are supposed to be protecting. Teams are given BSD-based servers. Starting out, all teams have identical software, and identical configs, minus IP addresses. In a few minutes, kenshoto will give you a connection to the game network. You’ll be on the 10.69.8.0/255 network. The teams networks are 10.69.1.0/255 through 10.69.7.0/255. The servers they need to defend will always live at .1.

These servers will have two types of tokens on them. First is PUBLIC tokens, which anyone may read, but must be overwritten for you to score. Second is SECRET tokens, which you can overwrite or steal for points.

In a few minutes, we will be providing you with the following:

- A CD containing the contents of the jail file system for your reference.
- Authentication information for submitting SECRET tokens that you steal. Check the CD for more information.
- A program for submitting breakthroughs to kenshoto. It’s written in Python, and you’ll need to instll the SC module provided on the CD. Python 2.4 is required.
- A program called gentok.py that generates tokens you can use to overwrite other people’s tokens. It is on your CD. This script will work anywhere that runs Python. You can only get credit for a single generated token one time.
- A script for submitting stolen SECRET tokens, It is the subtok.py script that comes with your CD.
- A “totem”. You will need to present your totem in order for kenshoto to answer questions and so on. We may also demand to see it on request. If your totem is lost or stolen, you are pretty much fucked, so guard it carefully.

We also have an in-game auction site. You as a ronin will want to use this to your advantage. You can trade knowledge of vulnerabilities to teams for some of their tokens, for example. Visit eday.kenshoto.com to list an item.

On the whole, it is not a good idea to hold onto breakthroughs without submitting them (they’re worth mucho points for the first submitter, and the points scale down tremendously on subsequent submissions).

Be creative in using your social skills and other skillz to get tokens from teams. Remember that, while you’re competing against the other ronin, you are also competing against the teams. They have the advantage of more people, but they also have disadvantages, such as losing points for service downtime. Use these things to your advantage. Steal tokens, but also make it difficult for teams to get their services back up. Blackmail them for “protection” from this, by making them give you tokens. They shouldn’t mind too much, because it doesn’t directly hurt them to give you tokens, as you were going to gain on them anyway, and at least other people don’t gain on them...

GAME RULES

- Do not DoS opponents network connections or kenshoto boxes.
- You will receive points for submitting advisories and stolen SECRET tokens.
- You will receive points for overwriting tokens, even if they have been overwritten previously by other teams.
- You only receive points for an overwrite once per time we replace the key. Don’t overwrite keys in while(1) loops (doing so will result in massive penalties).
- Watch out for the amount of bandwidth you use ;-)
- Individuals may not join teams (though feel free to spy).
- Any decision made by a kenshoto member takes priority over these rules, and is final.
- People in the kenshoto gopher shirts cannot make decisions or answer questions, but may impart info or orders to you, and be used to enforce rules. They’ll chop your balls off, man!
- If you root a non-team (kenshoto) box via the network, you will receive massive points. It can be done, it’s just going to be ridiculously hard.
- However... if we catch you trying to hack us before you actually succeed, we will penalize you 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.