悟入户

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 other’s servers, and ultimately stealing or overwriting other teams’ tokens. If you’re a team, you must also defend your own server.

Team Setup Information

As a team, you will need to defend a BSD-based server, keeping up a large number of services that your users demand. In a few minutes, kenshoto will give you two ethernet connections, one to the game network and one for capture. You’ll also be receiving:

- A CD containing a tarball of your file system (reference material... we are already running this image for you), the IP address and login information for your machine, and other important network info.
- A metric ass-tonne of authentication information for dealing with various services... For example, your user name and password 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 run the appropriate setup. You will need Python 2.4, and will need to install the SC module (on the CD).
- A team “totem”. You will need to present your team totem in order for kenshoto to answer questions, handle requests for machine resets, and so on. If your totem is lost or stolen, you are pretty much fucked, so guard it carefully.

Your machine will not be running any required services when the game starts, except for SSH. You may start services at your convenience by running /root/kinit.py.

You will not have any physical or console access to the machine you are guarding. You will not be able to install your own OS build. If your machine gets badly p0wn3d, and you want us to reset to its original state, we will do so (if you present us your totem). We suggest you write scripts to lock down the virgin install and then start services, as you learn what problems you need to fix.

To generate tokens that you can use to overwrite other people’s tokens, use the gentok.py script, which is on your CD. This script will work anywhere that runs Python. You can only get credit for a single generated token one time.

To submit stolen SECRET tokens, use the subtok.py script that comes with your CD. You can run this script from client boxes, or from your server.

When you submit a breakthrough, the information will not become public. You will know we received and accepted your breakthrough when you see it appear in /ADVISORIES on your file system. If someone manages to root your server, these will be accessible. 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).

We also have an in-game zero-day auction site. Visit eday.kenshoto.com.

Of the services you have to run, some we know have vulnerabilities, and some we believe do not. You still have to keep them up to the satisfaction of our uptime polls. Yes, you can script services, but our service polls can get sophisticated and new polls/twists may appear during the game, so be careful not to disturb any functionality that we explicitly check for. There is at least one back door, and our polls do not check for them.

GAME RULES

- Do not DoS any network connections or any 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 will lose points for network services not being available.
- You only receive points for an overwrite once per polling cycle (defined by how often we replace the key). Cycles are a minimum of 1 minute long, so don’t overwrite keys in while(1) loops (doing so will result in massive penalties).
- As in previous years, watch out for the amount of bandwidth you use ;-)
- Once you are on a team, you can’t join another team (though feel free to spy).
- Individuals may not join teams.
- 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.