King of the Hill

> ⚠️ **CAUTION**
>
> King of the Hill Challenges are only available on Hosted or Self-Hosted Enterprise CTFd Instances

King of the Hill (KotH) Challenges involve a user taking control of a server and leaving their identifier on a specified target server/application. This indicates which user/team has control of the server. Then the scoring engine (CTFd) is supposed to monitor this target and award the user/team some amount of points.

CTFd Enterprise provides the KotH Challenge Type which makes it possible to run this type of challenge on CTFd. Check out this tutorial on how to setup a King of the Hill challenge.

User View

When users view the KoTH challenge, the modal shows the user's **identifier** and **target server/application**. In the example below, it's `user#8` and `http://<server>:5000`, respectively.

The user identifier is automatically generated by CTFd for each user. This is what users would leave on a specified target server/application in order for CTFd to identify the user/team and award them with points.

The target server/application is manually added by the admin in the **Connection Info** upon configuring the challenge. This is the server/application that users compete to take control of.

A King of the Hill Challenge

Sample description for King of the hill challenge

Your user identifier is user#8

Leave your identifier on the target to show that you control the server. You'll get more points the longer you control the server.

http://<server>:5000

Submit

Admin View

Challenge Configuration

In order for CTFd to determine from time to time who is the current owner of the target server/application, and award points to the winning user/team, the KoTH Challenge Type has to be configured so that CTFd can send requests and receive responses from the KoTH Agent Server.

- URL - The URL that CTFd will check to determine which user/team is currently in control of the server
- API Key - An API Key header sent to the URL provided above, which authenticates the request
- TLS/SSL Certificate - A TLS/SSL certificate that's used to encrypt communication to the target server
- Interval - How often to check the server
- Reward - How many points to give to the user/team that controls the server for each check
- Connection Info - The URL of the target server/application

URL
URL that CTFd will check to determine what team/user owns the server

API Key

API key sent to the check URL to authenticate

TLS/SSL Certificate

SSL Certificate used by agent to encrypt communication

Interval

How often (in seconds) that CTFd will check for who owns the server

Reward

How many points the team/user gets for each check award

Connection Info

Use this to specify a link, hostname, or connection instructions for your challenge.

Status Check

Once the **URL** of the KoTH Agent Server and **Interval** have been specified in the challenge configuration, CTFd will start sending requests to the URL specified (most likely in the `/status` endpoint of the agent).

The responses from the agent can be checked using these two buttons in the challenge configuration page, which shows a pop-up box with the following JSON responses.
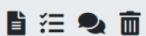
A King of the Hill Challenge

king of the hill
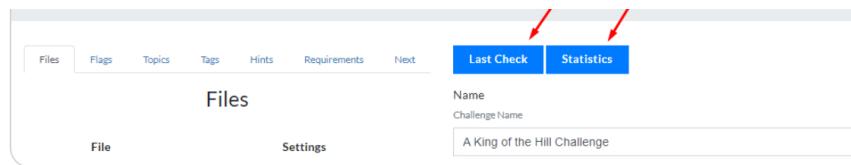
koth

visible

None points

Last Check

```
{
  "data": {
    "award_id": 1,
    "challenge_id": 13,
    "date": "2022-09-24T07:35:01Z",
    "error": null,
    "team_id": 1,
    "user_id": 2
  },
  "success": true
}
```

Statistics

```
{"count":255315,"team_id":null}
{"count":18321,"team_id":1}
```

KotH Agent Server

The KoTH Agent Server is an open-source agent, provided by CTFd, to run alongside the KoTH Challenge Type and the target server/application. The agent monitors the target server/application for the current owner and simultaneously listens and responds to HTTP requests.

This tutorial shows how to setup the KoTH Agent Server with an example target server/application.

Agent API Specification

- Swagger YAML
- API Documentation

Agent CLI Usage

```
❯ ./agent -h
Usage of ./agent:
  -apikey string
        API Key to authenticate with
  -certfile string
        SSL certificate file
  -certstring string
        SSL cert as a string
  -file string
        text file to watch for server ownership changes (default "owner.txt")
  -health-cmd string
        command to run when asked for a healthcheck (default "true")
  -help
        print help text
  -host string
        host address to listen on (default "0.0.0.0")
  -keyfile string
        SSL key file
  -keystring string
        SSL key as a string
  -origin string
        CIDR ranges to allow connections from. IPv4 and IPv6 networks must be specified
  -owner-cmd string
        command to run when asked for an owner
  -port string
        port number to listen on (default "31337")
```

Was this page helpful?   👍   👎

Share your feedback

Docs

Documentation

Community

MajorLeagueCyber [↗]

Twitter [↗]

More

Blog

GitHub [↗]

Copyright © 2025 CTFd LLC. Built with Docusaurus.