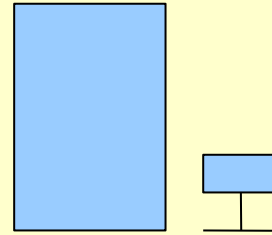
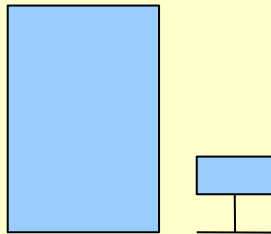


CTF изнутри

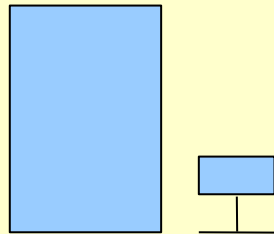
Jury server
*checking system,
flag reception,
scoreboard,
advisories,
announcements*



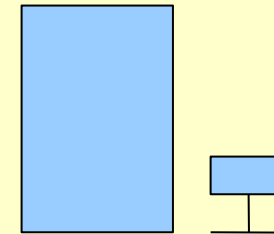
Team1 server
service1, service2, ...



Team2 server
service1, service2, ...



TeamN server
service1, service2, ...



Checking system

- Store <team> <service> <flag> <id>
- Retrieve <team> <service> <flag> <id>
- FunctionalityCheck <team> <service>
(flag: [0-9a-f]{32}, id: [0-9a-f]{16})

Service status

- OK
- Error
- Wrong flag
- Network down
- Garbled output

Flag reception

- Нельзя посылать свои флаги
- Флаги со временем устаревают
- Нельзя посылать флаг, если на вашем сервере сервис, с которого вы украли флаг, лежит

Info services of Jury server

- Scoreboard
- Advisories
- Announcements

Типы сервисов

- Web
 - php, sql, perl, jsp, python, ruby
 - javascript, xsl
- Скриптовые языки
 - perl, python, ruby, haskel
- Компилируемые языки
 - c, c++, java
- Reverse engineering
 - compiled c, c++, asm, python
- Устаревшие/эзотерические языки
- Quests

Роли в команде

- Капитан
- Администратор
- Специалисты
 - patching
 - exploiting
 - общая подготовка

Выигрышные стратегии

- Максимальная автоматизация
 - сбор и постинг флагов
 - watchdog`и на сервисы
 - обнаружение вторжений
 - резервное копирование (в том числе snapshot`ы)
- Набор готовых утилит
 - различные шеллы и руткиты
 - сниферы
 - фильтрующие прокси

Этика

- Атаки типа DOS
- Совершение запрещенных правилами действий от имени другой команды