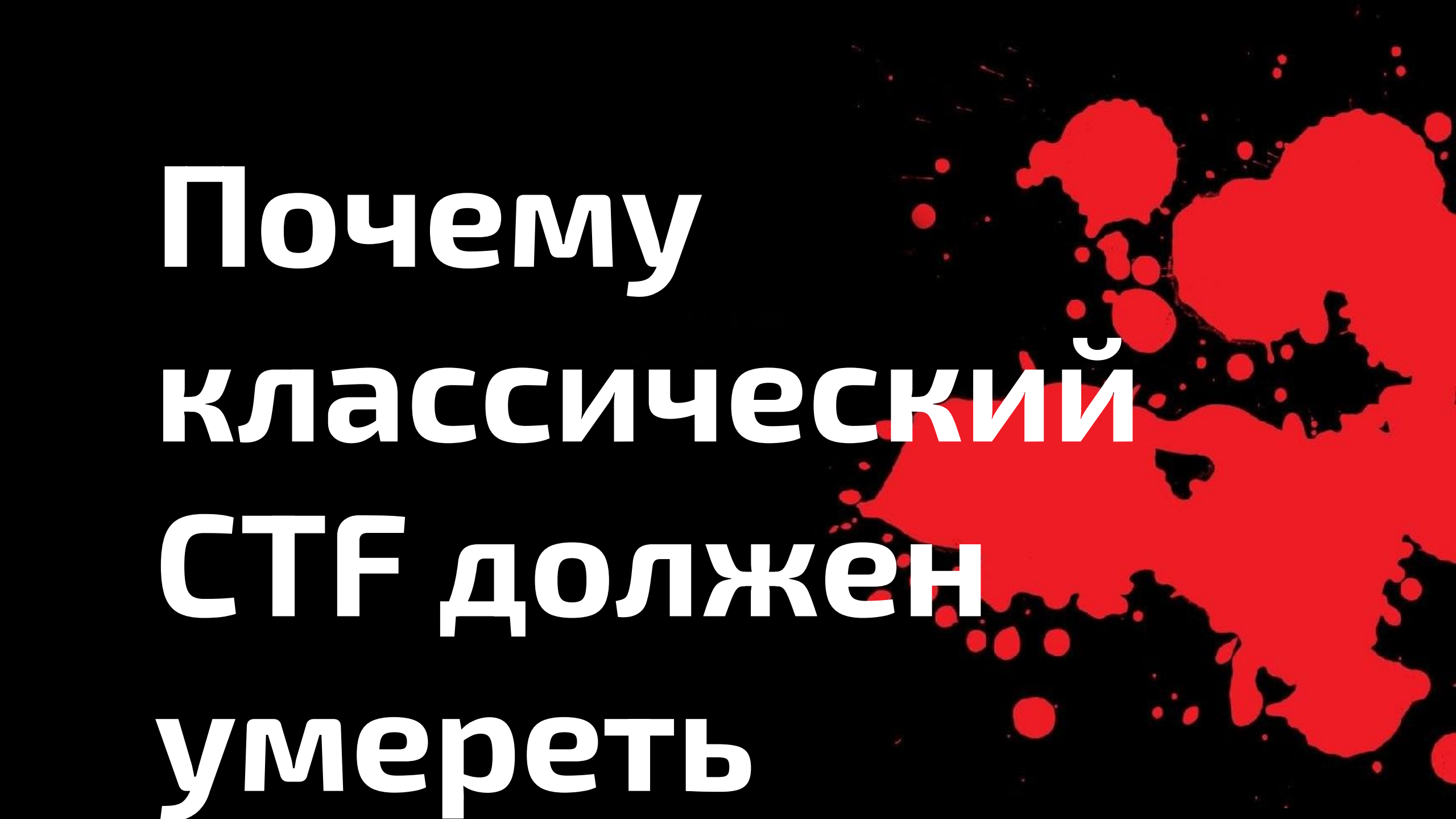
Почему классический CTF должен умереть



Ты кто?

Андрей Гейн

Хакердом, Екатеринбург

RuCTF 2010–2014

RuCTFE 2010–2012, 2015

QCTF Starter

QCTF School

Видео-курс по CTF

training.hackerdom.ru

vk.com/hackerdom


Roland
FR-1B
diatonic
V-Accordion

Классический

Тасковый

Задачи классического CTF

- Аудит системы, поиск уязвимостей
- Неизвестные ОС, языки программирования, стеки технологий
- Эксплуатация уязвимостей
- Системное администрирование

В правилах пишут

- запрещено проводить деструктивные атаки
- генерировать неоправданно большой объём трафика

Проблемы классического CTF

Медленная сеть

Поднять все виртуалки у себя?

Слабые компьютеры

64-bit, 2 cores, 2 Gb RAM, 20 Gb HDD

Сильные соревнуются,

кто сильнее побьёт слабых

Эксплойт-фермы — зло

только отнимают время и
нагружают сеть

Тренироваться невозможно

- для запуска проверяющей системы нужно владеть кунг-фу
- ОС, языки и технологии устаревают
- для тренировки нужно много человек

Крадут флаги через уязвимости в других сервисах

На серверах остаются следы

Можно смотреть, как тебя атакуют

и тупо повторять

Можно заполнить свой сервер фальшивыми флагами

Можно заполнить чужой сервер фальшивыми флагами

Кстати, DoS

Простые уязвимости или сложные?

Незапланированные уязвимости

IDS и IPS

закрывают половину уязвимостей

Фильтруем чекер

NAT, User-Agent, задержки, «умный рандом»

Проверяющая система — сложная штука

Хаотические результаты

И многое другое...

- Непонятно, что является флагами
- Сервис работает, а чекер говорит DOWN
- Флаги крадутся вручную
- Разные по сложности сервисы оцениваются одинаково

Хороший классический CTF — штучный товар

USCB iCTF

Критикуя предлагай

Атака + защита

К защите допускать только после успешной атаки

Команде не надо делать сервер доступным из интернета

Доказательство атаки

эксплойт

Эксплойт
натравливается
на сервер с флагами

Очки за атаку

Жюри может накладывать частичные защиты

Защита: ограниченный доступ на сервер, эксплойты жюри

Очки за защиту

Если выдержала, защита атакуется эксплойтами других команд

Дополнительные очки за защиту

Пробивание защиты, не пробиваемой эксплойтами жюри

Бонусные очки за атаку

Защита от эксплойта, который пробивает другие защиты

Бонусные очки за защиту

Технические сложности

- Нужно хранить построенные защиты
- Нужно хостить TEAMS * SERVICES виртуалок для построения защиты
- Нужны новые проверяющие системы

Минусы

- Меньше интерактивности
- Меньше системного администрирования

Медленная сеть

Слабые компьютеры

Сильные соревнуются,

кто сильнее побьёт слабых

Эксплойт-фермы — зло

только отнимают время и
нагружают сеть

Тренироваться невозможно

- для запуска проверяющей системы нужно владеть кунг-фу
- ОС, языки и технологии устаревают
- для тренировки нужно много человек

Крадут флаги через уязвимости в других сервисах

На серверах остаются следы

Можно смотреть, как тебя атакуют

и тупо повторять

Можно заполнить свой сервер фальшивыми флагами

Можно заполнить чужой сервер фальшивыми флагами

Кстати, DoS

Простые уязвимости или сложные?

Незапланированные уязвимости

IDS и IPS

закрывают половину уязвимостей

Фильтруем чекер

Проверяющая система — сложная штука

Хаотические результаты

И многое другое...

- Непонятно, что является флагами
- Сервис работает, а чекер говорит DOWN
- Флаги крадутся вручную
- Разные по сложности сервисы оцениваются одинаково

Хороший классический CTF — штучный товар


REVOLUTION

Почему классический CTF должен переродиться