

Санкт-Петербургский государственный университет информационных технологий, механики и оптики

Кафедра БИТ

CIT CTF

Как придумать, организовать и
провести соревнования по
компьютерной безопасности

Capture the flag

Соломатин А. Ю. группа 4131
solomatin@gmail.com

КТО МЫ?

- CIT CTF
- Dr. Giovanni Vigna и iCTF
- RuCTF
- HackInTheBox
- HC's Capture the Flag
- C.I.P.H.E.R.
- РусКрипто
- Codegate

При подготовке к данному докладу был составлен небольшой FAQ.
Команда HC's Capture the Flag в помощь другим командам
опубликовала его по адресу <http://ctf.hcesperer.org/orga.html>.

Полная версия и презентация доступна на сайте <http://ctf.ifmo.ru>.

Сложности.

- Поддержка:
 - Университета или организации.
 - Хорошее оборудование и пропускная способность Интернет канала.
 - Мотивированные и квалифицированные люди, готовые работать на СТФ.
- Организация людей:
 - Разработчиков
 - Спонсоров.
- Разработка концепции игры одновременно сложной, в тоже время, интересной и захватывающей.
- Создание безупречной автоматической системы начисления баллов, которую невозможно обмануть.
- Давление времени.
- “СТФ - это целый комплекс небольших подзадач, которые необходимо органично собрать воедино и обеспечить безотказную работу всего комплекса на протяжении всей игры.” – Илья Зеленчук, организатор RuCTF

Основные технические проблемы, которые всегда случаются.

CTF на базе университетов намного проще поддерживать с технической точки зрения из-за доступности хорошей и распределенной технической базы.

- В любой сложной системе, все что может сломаться, обязательно сломается, и к этому нужно быть готовым. Не должно быть проблем с переносом игры на запасные backup сервера, и этот процесс должен быть максимально автоматизирован с помощью самописных shell скриптов.
- Основная проблема – это железо и время, требуется соответствующее «кашерное» оборудование.
- Проблемы с сетевой инфраструктурой.
- Авторы сервисов и заданий почти всегда не успевают реализовать свою разработку в необходимые сроки.
 - На сайте NC's Capture the Flag есть хорошее руководство по написанию сервиса для CTF и руководство по написанию хорошего сервиса для CTF. Каждая ошибка, описанная в этих руководствах, была допущена на практике.
- Советы:
 - Все новое необходимо тщательно тестировать и проводить моделирование процесса игры.
 - В любой момент времени в жюри должно быть как минимум 2 человека, готовых помочь командам.
 - Не допускать ситуации, когда только один человек может произвести определенные действия на игре.

Необходимое аппаратное и программное обеспечение.

- Open-source + самописное.
- Из коммерческих VMWare Workstation для создания образов. Для запуска VMware Player.
 - Среди организаторов становится популярным использование VirtualBox.
- Для организации сети самым лучшим решением является OpenVPN.
- Gameserver - на любом языке программирования. В сети также есть и готовые варианты.
 - Многие организаторы создают gameserver с использованием функциональных языков программирования, например Erlang.

Пример успешной конфигурации оборудования из расчета на 6 команд для offline CTF.

• Игровой сервер

- Два четырехъядерных процессора Intel® Xeon® серии 5345
- DDR2 FB DIMM 667MHz 2Gb x 4шт. = 8Gb
- RAID контроллер SAS
- 1 SATA диск

• Сервер БД

- Два четырехъядерных процессора Intel® Xeon® серии 5500
- DDR3 DIMM 1333MHz 1Gb = 6Gb
- RAID контроллер SAS
- 2 SAS диска

Сетевое оборудование из расчета на 6 команд



1 Коммутатор Cisco Catalyst 3560



6 Wifi коммутаторов



Патч-корды

Общая настройка.

- Довольно сложная и качественная система, которая охватывает все компоненты информационной системы.
 - Сетевое оборудование
 - OS.
- Часто сложность заключается не в самой настройке, а в поиске квалифицированных специалистов, способных качественно сделать необходимую настройку оборудования.
- У многих команд настройка для CTF усложняется с каждым годом.
 - Отдельные задания требуют отдельных хостов, в связи с чем, приходится запускать немалое количество виртуалок.
 - Часто все хосты на всех играх виртуализируют, потому что так легче делать откаты, копии, проводить тестирование и добавлять изменения во время игры.

Скорость сети и расход трафика.

- Минимум 100Mbit/sec, лучше 1000Mbit/sec.
- Примерно 10-100 Gbytes трафика может быть израсходовано, это зависит от концепции игры.
- Если играть только в таски, то скорости в 10 Мбит/сек вполне хватит.

Команда.

- В среднем 5-6 человек.
- 1 разработчик на 1 сервис или 1-2 таска.
- Хорошая организация у команды RuCTF:
 - 1 разработчик на 1 сервис
 - 2 разработчика на проверяющую систему
 - 1 ответственный за сборку игрового образа
 - 2 сетевых администратора
 - 1 общий лидер команды
 - 2-4 человека на организационные вопросы.

Самая значимая статья расходов.

- Хорошее техническое оснащение.
- Время.
- Люди.

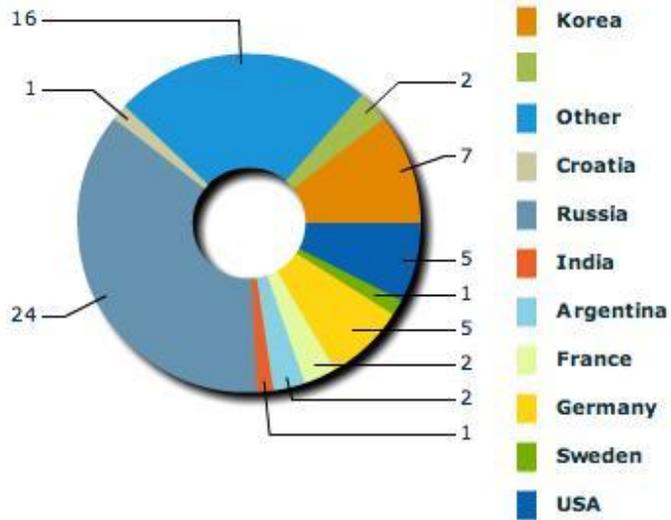
Средняя стоимость СТФ.

- Хорошая современная инфраструктура зарубежных организаторов составляет от 10 – 15 тыс. EUR.
- Основные деньги тратятся на оборудование и Интернет доступ с хорошей пропускной способностью.
- Потребление электроэнергии составляет незначительную сумму.

Спонсоры.

- Примерно 2 – 3 компании, готовые активно спонсировать соревнования.
- Спонсорство обычно проявляется в поддержке техническим оснащением и призами.
- За рубежом все проще, поддержку в основном оказывает университет, на базе которого проводятся соревнования.

CIT CTF 2010



- 64 команды
- 47 приняли активное участие

Наш setup

- Сервер на базе Supermicro.
- Gameserver с применением LAMP.
- Трафик – 1 Gbyte трафика.
- MySQL сервер 542,871 запрос за 24 часа, 194 в минуту.
- Рейтинг заданий показал оценку – 4.
- 20 часов на задания.



WINNING TEAMS

1. Nibbles

2. SiBears

3. HackerDom

Team name	Country	Time spent	TOTAL
1. Nibbles	<i>France</i>	19:26:15	3600
2. SiBears	<i>Russia</i>	22:04:46	3600
3. HackerDom	<i>Russia</i>	17:40:15	3400
4. gn00bz	<i>Croatia</i>	16:50:19	3200
5. ENOFLAG	<i>Germany</i>	19:20:56	3100
6. FlexSurfing	<i>Germany</i>	19:26:25	3100
7. WildRide	<i>Russia</i>	21:34:06	2700
8. PeterPEN	<i>Russia</i>	22:31:19	2600
9. Big-Daddy	<i>France</i>	21:17:28	2400
10. 0x28 Thieves	<i>USA</i>	22:36:14	2400
11. OldEur0pe	<i>Germany</i>	15:39:49	2300
12. WildGophers	<i>Russia</i>	21:57:45	2200
13. VLGU	<i>Russia</i>	23:50:28	2200

Заклучение

- *“Create a “story” behind the CTF. I think that the iCTF is the only competition that attempts to do so.” - Dr. Giovanni Vigna*