Уральский государственный университет им. А.М. Горького
математико-механический факультет и
РУНЦ «Информационная безопасность»
г. Екатеринбург, Россия

Соревнования CTF

В компьютерной безопасности термин CTF (Capture the flag, захват флага) означает командные соревнования, целью которых является оценка умения участников защищать компьютерных систем и проводить аудит их безопасности. Каждая команда получает выделенный сервер или небольшую сеть для поддержания ее функционирования и защиты. Во время игры команды получают очки за корректную работу своих сервисов и за полученную информацию (флаги) с серверов противников.

Существует несколько причин, по которым имеет смысл проводить подобные игры среди студентов. Одна, и наиболее важная из них, это то, что, в отличие от стандартных аудиторных занятий, они позволяют обучить специалистов по компьютерной безопасности защите компьютерных систем в условиях приближенных к реальности. Подготовка подобной игры требует от организаторов проведения большой работы и дает ценный опыт для каждого из них, а участники, то есть студенты, получают новые навыки, необходимые специалистам по компьютерной безопасности, и учатся работать в экстремальных условиях.

Удачное выступление на соревнованиях поднимает репутацию участников среди специалистов по компьютерной безопасности, а также демонстрирует их уровень знаний в работе со сложными системами. Опыт показывает, что такой стиль обучения студентам нравится больше, чем традиционные курсы и они готовятся с большим интересом.

Основной целью игры является симуляция компьютерной сети находящейся под постоянной атакой, чтобы посмотреть, как участники игры справятся с этой ситуацией. Конечно, до начала игры участники как минимум должны иметь общее представление о том, как защищать компьютерную систему. Более того, подобные игры позволяют получить навык не только в защите, но и атаке, что необходимо для высококлассного специалиста.

На игре участники группируются в команды, каждой из которых предоставляется сервер. Опыт показывает, что наиболее эффективные команды состоят из 7-10 человек. Меньшие команды просто не успевают за более крупными, а слишком большая команда менее продуктивна из-за больших временных затрат на внутреннюю организацию. Использование команды средних размеров делает возможным одной группе студентов разбиться на 3-4 команды и еженедельно проводить тренировки.

Игра может проводиться как очно, так и удаленно по сети Интернет. Первые и на данный момент самые популярные очные соревнования проводятся на международной хакерской конференции DEFCON. Первые удаленные международные межвузовские соревнования iCTF UCSB были проведены университетом Калифорнии, город Санта-Барбара в 2004 году. Другими известными соревнованиями CTF являются C.I.P.H.E.R (Аахенский Технический Университет, Германия.), UralCTF (Екатеринбург/Челябинск, Россия). В 2008 году были впервые проведены российские очные соревнования RuCTF, организаторами которых выступили УрГУ, РУНЦ «Информационная безопасность» и команда ХакерДом.

ХакерДом

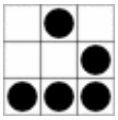
ХакерДом - это команда, образовавшаяся в УрГУ в 2005 году, основным направлением деятельности которой является компьютерная безопасность. Состав команды 14 человек включая студентов 1-4 курсов, а также выпускников, магистрантов, аспирантов и преподавателей. Все магистранты в команде являются преподавателями. На протяжении всего времени существования команда проводит еженедельные семинары «Секреты ХакерДом'а» где выступают студенты с разных факультетов и университетов. За это время на семинаре прозвучали такие темы как «Rootkit в ОС Windows NT и GNU/Linux», «BotNet (война хакеров)», «Google hacking», «Социальная инженерия», «Протокол SNMP. Проблемы безопасности» и многие другие. В последствии, часть докладов были представлены на различных конференциях по компьютерной и информационной безопасности.

В качестве проверки своих навыков команда ХакерДом участвует в различных международных CTF, в частности на iCTF UCSB, C.I.P.H.E.R. и DEFCON. В 2007 году на соревнованиях iCTF UCSB команда заняла 3 место из 35 команд со всего мира, а в 2008 году на соревнованиях C.I.P.H.E.R. стала первой.

Участники команды занимаются преподаванием в УрГУ, проводят факультативы в СУНЦе и участвуют в исследовательских проектах.

CTF в России

В 2006-2007 годах совместными усилиями студентов, аспирантов и преподавателей УрГУ и ЧелГУ было проведено несколько соревнований CTF регионального масштаба.



В 2008г. при поддержке Уральского государственного университета, а также ряда спонсоров команда ХакерДом провела первые открытые межвузовские соревнования по защите информации RuCTF. Участие приняли:

- Томский государственный университет (команда SiBears);
- Южно-Уральский государственный университет и Челябинский государственный университет (Smoked Chicken);
- Курганский государственный университет (Гарде);
- Томский государственный университет систем управления и радиоэлектроники (KEVA);
- Курский государственный технический университет (eXpl0it);
- Уфимский государственный авиационный технический университет (Reboot);
- Уральский государственный университет (HackerDom и НИИ ЧАВО).

Помимо команд были независимые наблюдатели из 11 различных ВУЗов. Дополнительная информация по этому соревнованию доступна на сайте http://www.ructf.org.

Весной планируется провести очередные соревнования RuCTF. Информация об этом появится на сайте немного позже. Основная часть правил и способ проведения соревнований не изменится. Для того, что бы новые команды лучше узнали о CTF в феврале месяце будет проведена пробная игра по сети Интернет.

Игра под ключ

На первых соревнованиях RuCTF мы обнаружили, что многие команды, впервые принимающие участие в подобной игре сильно отставали от более опытных соперников. Дело было не в мастерстве, а в опыте. И для того, что бы начать качественные и интенсивные тренировки достаточно один-два раза поиграть в CTF.

По этой причине команда ХакерДом предлагает «Игру под ключ» - это комплект, включающий:

- Семинар, на котором мы детально расскажем о CTF и поделимся своим опытом подготовки и участия в международных соревнованиях;
- Пробная тренировка;
- Игра в CTF;
- Разбор игры;

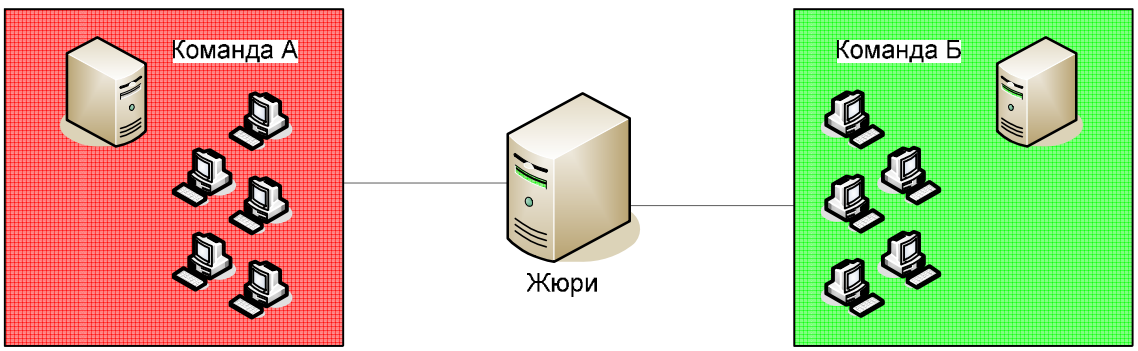
Все эти мероприятия проводятся на базе ваших ВУЗов с участием студентов.

Для организации пробной игры требуется минимум две команды, состоящие из 5-7 человек. В случае нехватки людей, команды можно будет организовать по 3-4 человека. Желательно, если команды будут размещаться в одной аудитории с компьютерами подключенными в локальную сеть. Число компьютеров в каждой команде должно быть не менее числа участников плюс один дополнительный для сервера. Вместе с командами в игре участвует жюри, на компьютере которых установлена проверяющая система (checker). Она следит за работой сервисов у команд, регистрирует успешную защиту и атаку сервисов, ведет подсчет баллов. Соответственно, для жюри требуется отдельный компьютер.

Предположим, у вас есть две команды состоящие из 5 человек каждая, тогда, для игры понадобится:

- 10 студентов;
- одна компьютерная аудитория;
- 13 компьютеров.

Ниже приведен пример схемы локальной сети для проведения тренировки или игры:



С предложениями и вопросами обращайтесь:
Зеленчук Илья Валерьевич (email: ilya@hackerdom.ru)

Полезные ссылки

1. DEFCON CTF - https://www.kenshoto.com/
2. iCTF UCSB - http://www.cs.ucsb.edu/~vigna/CTF/
3. C.I.P.H.E.R. - http://www.cipher-ctf.org/
4. UralCTF - http://www.hackerdom.ru/CTF
5. RuCTF – http://www.ructf.org
6. ХакерДом – http://www.hackerdom.ru