городов, как Калининград, Санкт-Петербург, Москва, Казань, Самара, Томск и другие.

Параллельно с финалом RuCTF проходила школа CSE-Days.Theory'2011, тема которой была обозначена как "Информационная безопасность и криптография". Все финалисты автоматически становились участниками школы и в течение трех дней обсуждали вопросы защиты информации, хэш-функции, задачи криптоанализа и теории чисел. А слушатели школы имели возможность посмотреть и принять участие в мероприятиях, проводимых в финале RuCTF'2011.

Описание соревнований RuCTF

RuCTF – это командные соревнования по защите информации, целью которых является оценка умения участников защищать и атаковать компьютерные системы. Соревнования проводятся по международным правилам CTF.

Capture The Flag – игра, в

которой несколько команд соревнуются друг с другом. Каждая команда получает от жюри сервер с предустановленным набором уязвимых сервисов. На момент начала игры серверы команд идентичны. Задачи участников: поддерживать свои сервисы в рабочем состоянии, предотвращая попытки вторжения, проводить атаки на серверы других команд с целью "захвата флагов". Командам необходимо обнаружить уязвимости на своем сервере и попытаться закрыть их, не нарушив работоспособности сервисов. В то же время, используя знания о найденных уязвимостях, становится возможным провести атаки на серверы других команд. При проведении атак на сервер команда должна обойти механизм безопасности сервиса и "захватить флаг" (некоторую приватную информацию), ассоциированный с данным сервисом. За отправку полученных "флагов" на сервер жюри команды получают баллы.

Во время игры жюри проверяет у всех команд корректное функционирование сервисов, устанавливает новые "флаги" и проверяет наличие уже установленных, а также отслеживает, на какие сервисы были проведены атаки, принимая захваченные "флаги" от команд.

Баллы начисляются команде:
- за корректное функционирование собственных сервисов;
- за захват флагов с сервисов других команд;
- за описание найденных уязвимостей, способов их исправления и использования;
- за выполнение дополнительных заданий;
- особым решением жюри.

Во время игры командам запрещается:
- проводить атаки на серверы жюри и проверяющую систему;
- проводить фильтрацию команд-противников по IP-адресам или любым другим способом;
- генерировать неоправданно большой объем трафика;
- проводить DoS с генерацией большого объема трафика;
- проводить деструктивные атаки на серверы команд (например, "# rm –rf /").

Во время игры командам предоставляется доступ в Интернет, а также разрешается использовать любое количество компьютеров и сетевого оборудования не выше второго уровня. Организаторы могут предоставить на время соревнований по одному компьютеру для каждого участника. Каждой команде предоставляется заранее настроенный маршрутизатор с учетными данными.

Более подробно с правилами проведения соревнований можно ознакомиться на сайте соревнований (http://www.ructf.org/).

DEFCON

В этом году впервые российская команда приняла участие в финале международных соревнований по информационной безопасности DEFCON 19 CTF, прошедших с 4 по 7 августа этого года в Лас-Вегасе (штат Невада, США). По итогам, объявленным организаторами 12 августа, наша команда заняла 4-е место из 12 команд, вышедших в финал (http://ddtek.biz/). Стоит отметить, что за 19 лет это первая российская команда, которая смогла пробиться в финальную часть CTF-соревнований конференции DEFCON.

Полуфинальные отборочные соревнования DEFCON 19 CTF Quals проходили в сети Интернет с 3 по 6 июня этого года, участие в них приняло более 650 команд со всего мира, из них 280 завершили игру с ненулевым результатом. Российская команда также была четвертой и в отборочных соревнованиях. Занятые места в двух турах стали символичными. В состав сборной команды вошли четыре сильнейшие CTF-команды России: HackerDom (Уральский федеральный университет), LeetMore (Национальный исследовательский университет информационных технологий, механики и оптики), SiBears (Томский государственный университет) и SmokedChicken (Челябинский государственный университет). Участники сборной выбрали название команде – "IV".

Оргкомитетом RuCTF после такого успеха было принято решение о ежегодном формировании сборной команды для участия в международных соревнованиях по информационной безопасности. ●

DEFCON – крупнейшая ежегодная конференция хакеров, которая проходит в Лас-Вегасе (штат Невада, США). Большинство посетителей этого мероприятия – профессионалы в области информационной безопасности, исследователи, разработчики ПО и другие специалисты, так или иначе связанные с IT-сферой. Впервые DEFCON прошел в 1993 г. В 2006 г. это мероприятие посетило более 6500 человек, в этом году – более 15 000 участников. В рамках конференции проводится множество различных тематических конкурсов и соревнований. Одним из наиболее интересных и престижных является CTF (Capture The Flag). Участники DEFCON CTF сражаются не за сертификаты или материальные призы, а за уважение и признание сообщества. Само участие в финале – самая большая награда для специалиста по информационной безопасности. Отборочные соревнования проходят по сети Интернет. Их продолжительность – около 50 часов. На отборочных соревнованиях командам предлагается решить 25–30 заданий из различных областей IT, и только десятка лучших команд проходит в финал. Участникам команд необходимы широкие познания в сфере защиты информации и информатики, в особенности владение языками программирования, которые используются при написании сервисов, такими как C/C++, C#, Go, Haskell, Java, Perl, PHP, Python, Visual Basic и др., а также навыки в администрировании безопасности современных операционных систем и сетей. Более подробно о программе конференции можно узнать на сайте https://www.defcon.org/.

Организаторы RuCTF

Непосредственной организацией соревнований RuCTF занимаются РУНЦ УрГУ "Информационная безопасность" и клуб "Хакер-Дом" математико-механического факультета УрГУ. Команда разработчиков на сегодня уже составляет более 20 человек.

Начиная с 2008 г. соорганизаторами данных соревнований выступают Уральский государственный университет, Ассоциация защиты информации (г. Москва), Союз IT-директоров России (г. Москва), клуб профессионалов АСУ Урала (г. Екатеринбург). Финансирование соревнований проводится Фондом поддержки информационно-коммуникационных технологий (г. Москва), бюджет соревнований формируется за счет спонсорской поддержки частных компаний, работающих на рынке информационной безопасности России.

Ваше мнение и вопросы присылайте по адресу
infosec@groteck.ru