2008 Математические основы компьютерной безопасности № 2(2)
DOI 10.17223/20710410/2/17
УДК 681.322

О СОРЕВНОВАНИЯХ CTF ПО КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Д.Н. Колегов, Ю.Н. Чернушенко

Томский государственный университет

E-mail: kden@sibmail.com

Описывается концепция «CAPTURE THE FLAG» проведения соревнований по защите информации в компьютерных системах. Данный подход может быть использован для эффективного обучения по специальностям, связанным с обеспечением компьютерной безопасности.

Ключевые слова: *CTF*, *анализ защищенности*, *обучение*, *ролевые игры.*

В настоящее время известно несколько соревнований с концепцией «CAPTURE THE FLAG» (CTF) – DEFCON CTF, C.I.P.H.E.R, USF CTF и т.д. Далее речь пойдет о UCSB iCTF – международных распределенных соревнованиях по безопасности, организуемых Университетом Калифорнии Санта Барбары. Основная цель соревнований – проверка навыков проведения атак и защиты компьютерных систем (КС). В игре участвует неограниченное количество команд. Каждая команда имеет виртуальную сеть. В сети располагаются рабочие станции команды и защищаемый сервер, на котором запущено предоставляемое организаторами соревнований программное обеспечение, моделирующее уязвимую КС. Задача каждой команды – обеспечить состояние защищенности своих сервисов и атаковать сервисы других команд. Очки командам начисляются как за кражу флагов других команд путем компрометации сервисов, так и за защиту своих флагов. За доступностью сервисов и компрометацией флагов следит система подсчета очков (СПО).

Существует два основных вида CTF – CTF «с одной целью» и CTF «многие ко многим». В первом случае организаторами соревнований создается одна уязвимая система, а участники ее атакуют. Очки назначаются команде, сумевшей первой эксплуатировать уязвимость. Такой вид CTF часто организуется на конференции по безопасности DEFCON, которая сыграла значительную роль в популяризации игры. Во втором случае каждая команда и атакует, и защищается, имея в своем распоряжении копию уязвимой системы. Таким образом, выявление уязвимости позволяет команде защитить собственную КС и атаковать другие команды. Такой вид проведения CTF требует более сложную СПО.

CTF вида «многие ко многим» могут проводиться на уровне узла, когда все участники игры работают в одной системе, имея в своем распоряжении виртуальную (jail-подобную) систему, и на уровне сети, где все участники соединены по сети. У каждого из подходов имеются свои достоинства и недостатки. Достоинством CTF на уровне узла является то, что подсчет очков ведется путем простого чтения данных из специальных файлов различных виртуальных систем. К недостаткам следует отнести плохую масштабируемость и нереалистичность. CTF на уровне сети реалистичны, но для них более сложно обеспечить подсчет очков и соблюдение правил.

Турнир USCB CTF создан в 2003 г. сотрудником Университета Калифорнии Санта Барбары (UCSB) Джованни Вигна (Giovanni Vigna) на основе локальных соревнований DEFCON CTF. Основное отличие USCB CTF – распределенность и масштабность соревнований, а также неограниченное количество участников. Первоначально основные идеи игры использовались в процессе организации практических занятий по анализу защищенности компьютерных систем. В декабре 2003 г. были проведены первые соревнования среди 14 университетов США. В 2004 г. были проведены первые международные соревнования с участием команд из Норвегии, Италии, Германии, Австрии и США. Турнир 2005 г. проводился среди 22 команд, в том числе из Южной Америки и Австралии. С 2005 г. для обеспечения сетевого взаимодействия в процессе игры стали использоваться система Blending и GRE-туннели (до этого использовалась технология NAT), что значительно повысило реалистичность соревнований и упростило организацию.

В апреле 2008 г. на базе Уральского государственного университета им. А.М. Горького были проведены первые в России открытые межвузовские соревнования по защите информации с концепцией CTF – RuCTF-2008. Всего в игре приняло участие 9 команд из различных университетов России. Организаторами выступила команда Уральского государственного университета Hackerdom, имеющая большой опыт участия в соревнованиях подобного рода и занявшая 3-е место в UCSB CTF 2007.

Данная заметка написана по материалам из [1 – 3] и на основе собственного опыта участия авторов в UCSB CTF-2007 в составе команды Sibears Томского университета, впервые участвовавшей в подобных соревнованиях и занявшей в них 10-е место среди 35 команд университетов планеты.

1. Сетевая инфраструктура

Сеть USCB CTF (рис. 1) состоит из нескольких соединенных сайтов. Сайт включает одну или несколько сетей команд. Сайту выделяется множество немаршрутизируемых адресов класса B (например, 10.2.0.0/16), каждая команда в сайте получает множество немаршрутизируемых адресов класса C в соответствии с адресным пространством сайта (например, 10.2.1.0/24 и 10.2.2.0/24). В сети каждой команды размещены:

- узел team box (*tb*) с адресом x.y.z.1, обеспечивающий соединение с VPN-сервером игры main box (*mb*) через GRE-туннель;
- узел image box (*ib*, адрес x.y.z.2) с установленным ПО VMWare, предназначенный для эмуляции узлов vulnerable box (*vb*) и test box (*teb*), с адресами x.y.z.3 и x.y.z.4 соответственно. Узлы *tb* команд конфигурируются так, что любой исходящий трафик команд проходит через узел *mb*.

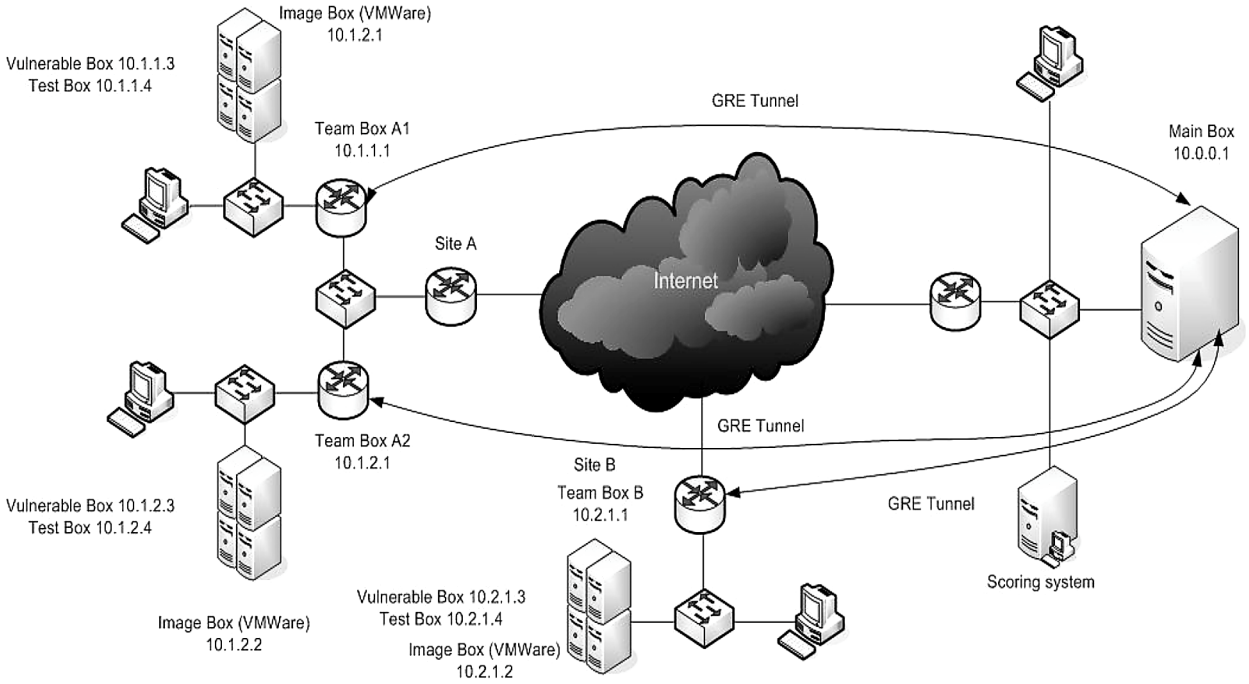

Рис. 1. Сетевая инфраструктура UCSB CTF

Узел *teb* предназначен для проверки готовности команды к соревнованиям, в процессе которой выполняются различные тесты, определяющие отсутствие фильтрации, прохождение дефрагментированного трафика, доступность сервисов, время прохождения датаграмм и т.д. Команды, не прошедшие проверку, к игре не допускаются до устранения несоответствий. Виртуальный узел *vb*, как правило, функционирует под управлением ОС GNU/Linux. Образ для *vb* создается организаторами соревнований и включает в себя несколько различных уязвимых сервисов (порядка 10), написанных на различных языках, и распространяется до начала игры в шифрованном виде.

2. Основные правила игры

В каждой команде назначаются faculty POC (point of contact) – лицо, ответственное за моральное поведение участников команды, и deployment POC – лицо, ответственное за функционирование сети и техническую подготовку команды. В соревнованиях участвуют только команды, имеющие отношение к образовательным учреждениям. Правила игры могут меняться, дополняться и уточняться. Основными правилами являются следующие:

- запрещены «массированные» DoS-атаки;
- запрещена генерация трафика DoS со взломанных узлов других команд;
- запрещены любые взаимодействия вне VPN;
- разрешены любые атаки на узлы VPN (в том числе и на рабочие станции);
- уязвимости должны быть устранены так, чтобы команды и система подсчета очков имели доступ к сервису, иначе очки с команды будут сняты;
- каждая команда должна поддерживать защищенность своих сервисов;
- продолжительность игры – 8 часов; первый час дается на подготовку, в течение которой атаковать другие команды запрещено.

3. Подсчет очков

Рассмотрим порядок действий СПО. В начальный момент времени t_0 СПО, используя служебную учетную запись, выставляет флаги для сервисов на узле *vb* каждой команды. Флаг – некоторый набор данных, ассоциированных с сервисом (например, `MTNzEwECA+hWjCb8t8/FgbEg/mSm1hbU231kjg=`). Затем в момент времени $t_1 = t_0 + q$ СПО пытается снова пройти регистрацию и получить доступ к сервису. Если регистрация проходит успешно и в момент времени t для $t_0 < t < t_1$ никто из команд не предъявил проверяемый флаг, то команде назначаются очки за защиту сервиса. Невозможность получить доступ к флагу расценивается как недоступность сервиса, и с команды списываются очки.

Считается, что команда A реализовала атаку в отношении некоторого сервиса команды B, если она может прочитать ассоциированный с этим сервисом флаг, сохраненный СПО, и затем предъявить его в заданный промежуток времени. Если флаг верный и еще не был обновлен СПО, то команде A начисляются очки за успешную атаку. Если несколько команд предъявили один и тот же флаг, то очки между ними делятся (простые уязвимости эксплуатировать легче, чем сложные). Временной интервал q свой для каждого сервиса.

Для предотвращения мошенничества в игре используется система *Blender*, задача которой – реализовать обращения СПО к сервисам от имени различных команд. Таким образом, значительно усложняется задача фильтрации входящего трафика с целью запрещения доступа к сервисам других команд и разрешения запросов от СПО. Общий принцип работы *Blender* заключается в сборе статистики о сетевом взаимодействии команд за некоторый период времени и затем генерации случайного раундового IP-адреса для доступа СПО к сервисам отдельной команды. Маскировка осуществляется с помощью технологии NAT на узле *mb*. Таким образом, СПО при проверке сервисов команды A с большей вероятностью будет использовать IP-адрес той команды B, которая наиболее активна в сетевом взаимодействии с A.

4. Организация игры

В команде должно быть не более 20 человек. Кроме оговоренных выше dpoc и fpoc, назначается или выбирается капитан команды. В процессе подготовки и проведения игры перед участниками стоят следующие практические задачи: администрирование КС, настройка межсетевых экранов и систем обнаружения и предотвращения атак, поиск уязвимостей в программном обеспечении (при наличии исходного кода и без него), сканирование сетей, написание и отладка эксплойтов и патчей, обнаружение вторжений, криптоанализ и др.

Сервисы, предоставляемые жюри в составе образа игры, пишутся на различных языках программирования – C, Java, Python, Ruby, PHP, Perl и др. Программное обеспечение может содержать ошибки, не позволяющие сервисам стартовать в системе или завершающие их через некоторое время.

Типовыми уязвимостями программного обеспечения являются SQL-injection, PHP-including, переполнение буфера, «гонки» и ошибки форматных строк. Встречаются также уязвимости конфигурирования КС – неправильные права доступа к каталогам, слабые и стандартные пароли.

Для каждой игры жюри придумывается легенда, объединяющая все задания и конкурсы (квесты) в одном тематическом плане, например: противостояние мафии и спецслужб, ограбление банка и т.д. В UCSB CTF-2007 для того, чтобы команда начала получать очки за защиту и атаку сервисов, ей было необходимо решить ряд головоломок различного уровня сложности. Пример такого задания – определение пароля, набранного злоумышленником, по видеофрагменту, записанному сотрудниками ФБР в результате наблюдения.

5. Организация обучения на основе CTF

На основе концепции CTF можно предложить пути для повышения эффективности подготовки специалистов по направлению анализа безопасности КС. Рассмотрим два варианта применения данной концепции. Первый из них заключается в проведении локальных CTF-соревнований со своей спецификой между командами обучающихся. Например, группа делится на 3 команды. Каждая команда по очереди выступает в качестве организаторов и жюри соревнований между двумя другими командами – придумывает замысел игры, создает образ игры, пишет уязвимые программы, осуществляет базовую настройку оборудования и т.д. Второй вариант состоит в предоставлении каждому обучающемуся своего образа CTF (локально или удаленно), на котором он сможет самостоятельно проводить анализ безопасности КС. Результаты выполнения заданий предоставляются организатору (преподавателю). Все образы CTF могут быть размещены на одном сервере при помощи современных технологий виртуализации КС. В последнем случае возникает непростая задача генерации образов CTF, так как все они должны быть в некотором смысле уникальными. Одним из решений может являться создание CTF-генератора, позволяющего генерировать множество различных образов из заданного шаблона. Данная задача в настоящее время исследуется автором USCB CTF Джованни Вигна.

ЛИТЕРАТУРА

1. http://www.cs.ucsb.edu/~vigna/CTF/
2. http://hackerdom.ru
3. http://ructf.org/