

С 24 по 26 апреля, в Уральском федеральном университете имени Б.Н. Ельцина прошли всероссийские межвузовские соревнования и конференция по информационной безопасности RuCTF-2015. В рамках этого мероприятия вопросы защиты информации и информационных технологий осветили представители таких компаний как: Positive Technologies, Kaspersky Lab, УЦСБ, ОАО «Мультиклет», Cisco Systems, ЦСР МО РФ и ИММ УРО РАН.

RuCTF-2015 примечательна широкой географией участников соревнований и конференции. Помимо представителей России, мероприятие посетили зарубежные гости из Китая из Белоруссии.

26 апреля состоялся финал RuCTF-2015. По правилам соревнований, участники получают идентичные серверы с предустановленным набором уязвимых сервисов. Задача участников — найти уязвимости, закрыть их у себя и воспользоваться ими для получения приватной информации (флагов) у соперников. Поскольку соревнования



проходили в Екатеринбурге, то было решено воспользоваться аппаратными решениями местной компании. Такой компанией стала «Мультиклет», которая предоставила свои отладочные платы для проведения соревнований.

В распоряжение каждой команды находился сервер под управлением ОС Linux на базе Raspberry Pi. С помощью Python было налажено взаимодействие с отладочной платой HW1-MCp04 от компании «Мультиклет», которая выступала в роли сервиса. На отладке был размещен кольцевой буфер на 1024 ключа, для выполнения функций шифрования и хранения ключей.

В каждом из серверов были заложены уязвимости. Уязвимости были на уровне логики и на уровне реализации. Уязвимости были связаны с методом и условиями хранения ключей, ограничения в размерах буферах, переполнения буфера, ошибками в протоколе.

Phoca PDF

Причем, используемый протокол в работе сервера и алгоритм были написаны специально для соревнований.

Для того чтобы победить, командам необходимо было набрать максимальное количество балов, начисление которых зависело от максимально набранных очков в каждой из категорий:

1) **SLA (team, service)** — это доля от прошедшего игрового времени, в течение которой данный сервис у данной команды был в состоянии доступности.

2) **FlagPoints(team, service)** – этот показатель определяет насколько хорошо команда умеет находить уязвимости в своем сервисе и закрывать их.

3) **Flags** - атаки на чужие сервера. (Количество украденных у противника флагов).



Команды в первую очередь должны определить, какая система у них используется в сервере, выяснить какие уязвимости есть на их собственном сервере и обеспечить должный уровень защиты путем внесения изменений в конфигурацию сервера. В дальнейшем можно было приступать к атакам на чужие сервера, воспользовавшись их уязвимостями.

Победителем соревнований стала команда Noobs4Win из Уральского федерального университета (Фото №3). Помимо приятных призов в виде комплектов компьютерной техники, команда получила почетный приз – переходящий кубок RuCTF, который, до следующей смены победителя соревнований будет храниться в стенах УрФУ.

???? ?3. ??????? Noobs4Win

Стоит отметить, что за соревнованиями подобного уровня пристально следят ведущие компании в области IT и информационной безопасности, поэтому для победителей и призеров этих соревнований появляется отличная возможность сделать важный шаг в карьере.

Phoca PDF



Итоги соревнований подытожил руководитель команды разработки RuCTF Михаил Вяцков: «Соревнования прошли достаточно успешно, за исключением небольших технических неполадок. Мультиклеты оказались очень интересны аудитории, тем более что разработаны они на Урале. Участники были удивлены этой технологией, им было любопытно работать с этими платами. Порадовало, что все команды добились определенного прогресса в соревнованиях. К сожалению ни одна их команд досконально не разобралась в специфике работы Мультиклетов, но общий принцип работы был освоен всеми. Организаторам соревнований можно дать высокую оценку за их работу. В следующем году мы попробуем повторить успех этих соревнований и, возможно, превзойти его. В том числе за счет новых продуктов от компании «Мультиклет».

Phoca PDF