ЦЕЛИ И ЗАДАЧИ ПРОЕКТА HONEYNET

Д.С. Кулябов*, А.В. Ульянов**

(РУДН*, E-mail − *.dharma@mx.pfu.edu.ru,
− **.aulianov@sci.pfu.edu.ru)

MAIN PURPOSES OF THE HONEYNET PROJECT

D.S. Kulyabov, A.V. Ulianov

The article describes the raising of network security level by analyzing the data received from the Honeynet, and methods of learning the tools and tactics of the black-hat community based on the results of the Honeynet Project Organization.

Одна из самых серьезных задач, которую приходится решать специалистам по безопасности, это сбор сведений, позволяющих обнаружить сетевых взломщиков, понять, как они действуют и почему. Раньше суть киберугрозы пытались выяснить, исключительно анализируя программы, использованные для проникновения: после того как произошел инцидент, единственные данные, которыми располагали специалисты, это информация, остававшаяся во взломанной системе. К сожалению, она крайне скудна и мало что может сказать об угрозе в целом. Очевидно, защититься и обезвредить врага, если о нем ничего неизвестно весьма трудно.

Проект Honeynet (http://*project.honeynet.org*) предлагает иной подход: «заманивать» хакеров в систему и анализировать их действия с самого начала. Такой метод эффективно дополняет хорошо известные технологии обнаружения и предотвращения вторжений.

Honeynet Project — это научная организация, занимающаяся исследованиями в области систем безопасности и специализирующаяся на изучении инструментария, используемого злоумышленниками, их тактики и мотивов [1]. Затем полученная информация и сделанные выводы предлагаются для ознакомления всем желающим. В состав организации входят специалисты по вопросам безопасности из разных стран, которые на добровольной основе предоставляют свои ресурсы для развертывания и изучения сетей-приманок, основное назначение которых стать объектом атаки ха-

керов. После каждого зарегистрированного инцидента собранная информация тщательно анализируется.

Идея создания honeypot разрабатывалась многие годы. Проще говоря, honeypot – это система, разработанная для того, чтобы на нее напали. После взлома хакер может ее использовать для разнообразных целей, например, для разработки механизма оповещения или для жульничества.

Honeynet – это инструмент исследования, представляющий собой сеть, созданную особым образом для того, чтобы ее взломали хакеры или, как их часто называют, «черные шляпы». После того как ее взломают, Honeynet можно использовать для изучения инструментов, тактики и мотивов сообщества черных шляп.

Создание и поддержка Honeynet зависит от двух важных составляющих – контроля и записи данных:

- после того как honeypot, входящая в Honeynet, взломана, необходимо остановить взломщика и убедиться, что honeypot не используется для взлома производственных систем в других сетях. Поток входящей и исходящей из Honeynet информации должен автоматически контролироваться, чтобы взломщик ничего не заподозрил. Эта часть работы называется *контролем данных*;
- нужно каким-то образом зафиксировать всю информацию, которая входит и покидает сеть, чтобы черные шляпы не знали о том, что за ними наблюдают. Кроме того, данные нельзя хранить на самих системах honeypot. Взломщик может найти эти данные, которые раскроют ему истинную суть Honeynet. Если хранить данные в локальных системах honeypot, они могут потеряться, когда взломщик разрушит или изменит систему. Эта часть работы называется *записью данных* [2].

За прошедшие несколько лет команда Honeynet Project определила распространенные инструменты, тактику и мотивы действия сообщества взломщиков и использовала полученные знания для создания общей методологии. Независимо от того, кем является пользователь и на какой ОС он работает, его система подвергается риску. Поняв механизм действий черной шляпы, можно лучше узнать своего врага и лучше понять возникшую угрозу [3,4].

Угроза заключается в так называемой методологии «script kiddie», когда система зондируется и взламывается через самые

уязвимые места (дыры). Методология «script kiddie» представляет собой путь наименьшего сопротивления. Побудительные мотивы человека могут различаться, но цель остается той же самой – получить контроль самым легким из возможных способов, обычно над большим количеством систем [4,5].

Тактика черных шляп очень проста: случайным образом сканируется Интернет в поисках определенных уязвимых мест, чтобы впоследствии их использовать [6]. Инструменты, используемые для нападения, сложны в разработке, но очень просты в применении. Для их создания требуются глубокие познания в области программирования низкого уровня, например, знание языка ассемблера и внутренних процессов ОС и разработки приложений. Лишь небольшой процент взломщиков владеет такой информацией [6,7].

Honeynet – это механизм изучения инструментов, тактики и мотивов сообщества взломщиков. Эта система уникальна тем, что ничего не имитируется. Вместо этого создается полностью контролируемая сеть из машин с ОС и приложениями, которые идентичны тем, что используются в производственной системе. После того как системы взломаны, они помогают не только понять действия черных шляп, но и определить риски и слабости, существующие во внешней среде. Основная ценность проекта Honeynet заключается именно в возможности обучения.

Литература

[1]. *Know Your Enemy: Honeynets*. - 2003. — http://project.honeynet.org/papers/honeynet/index.html.

[2]. *Know Your Enemy: A Forensic Analysis*. - 2000. — http://project.honeynet.org/papers/forensics/index.html.

[3]. *Know Your Enemy II: Tracking the blackhat's moves*. - 2001. — http://project.honeynet.org/papers/enemy2/index.html.

[4]. *Инструменты, тактика и мотивы хакеров. Знай своего врага*. - М.: ДМК Пресс, 2003. — 312 с.

[5]. *Know Your Enemy: The Tools and Methodologies of the Script Kiddie*. - 2000. — http://project.honeynet.org/papers/enemy/index.html.

[6]. *Know Your Enemy III: They Gain Root*. - 2000. — http://project.honeynet.org/papers/enemy3/index.html.

[7]. *Know Your Enemy: The Motives and Psychology of the Black-hat Community*. - 2000. — http://project.honeynet.org/papers/motives/index.html.