УДК 004.056.53

О целях и задачах проекта Honeynet

Д. С. Кулябов, А. В. Ульянов

Кафедра систем телекоммуникаций
Российский университет дружбы народов
Россия, 117198, Москва, ул. Миклухо-Маклая, 6

В данной работе рассказывается о методе повышения уровня сетевой безопасности посредством анализа данных, поступающих из «сети-приманки» Honeynet, а также о механизмах изучения тактики и мотивов сетевых взломщиков на основе результатов, полученных командой проекта Honeynet.

Ключевые слова: Honeynet, honeypot, blackhat, script kiddie, spam.

1. Введение

Одна из самых серьезных задач, которую приходится решать специалистам по безопасности, это сбор сведений, позволяющих обнаружить взломщиков и 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. Но как защититься и обезвредить врага, если даже не известно, кто этот враг?

Honeynet Project (`www.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 хакеров. После каждого зарегистрированного инцидента собранная информация тщательно анализируется.

К сожалению данный адаптивный подход практически не освещён в отечественной литературе (за исключением, может быть, перевода оригинальной документации [1, 2]). Поскольку это направление представляется весьма перспективным, предпринята попытка обзора основных теоретических и практических аспектов данной технологии.

2. Основные понятия и определения

В связи с отсутствием на данный момент общепринятой русскоязычной терминологии, в данной статье некоторые термины приводятся в оригинальной транскрипции.

Honeynet — это инструмент исследования, представляющий собой сеть, созданную особым образом для того, чтобы ее взломали хакеры.

Под термином *honeypot* подразумевается установка одной или нескольких систем, которые покажутся привлекательными для сетевых взломщиков и смогут также производить мониторинг практически всего, что в них происходит. Наблюдая за событиями, происходящими с honeypot, можно определить проблему и получить достоверную информацию о том, как взломщик вошел в систему и что творится во взломанной системе. Традиционно honeypot представляла собой одну систему, соединенную с существующей внешней сетью для того, чтобы привлечь нападающих к себе, и способную имитировать различные системы или уязвимые места [3].

Определённые проблемы возникают с термином *хакер*. Данный термин носит слишком неоднозначную и эмоциональную смысловую окраску. В связи с этим, в зарубежной литературе обычно используют более нейтральные термины *intruder* и *blackhat* [4]. Поэтому, наряду с термином *хакер* представляется оправданным использование термина *взломщик*.

Взломщики подразделяются на несколько категорий. Одни ищут и обнаруживают новые уязвимости, другие пишут инструментарий для использования найденных уязвимостей, а третьи применяют, порой бездумно, имеющийся в наличии инструментарий. Последняя категория взломщиков в англоязычной терминологии получила название script kiddie [5, 6]. Цель script kiddie — получить контроль самым легким из возможных способов, обычно над большим количеством систем.

Термин *спам* будет использоваться для обозначения нежелательных массовых рассылок, чаще всего — рекламного характера [7].

3. Honeynet — инструмент исследования

3.1. Понятие Honeynet

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

Разнообразные разработки позволяют создавать собственную honeypot. Среди них можно выделить Deception Toolkit (DTK) и Resource Mantrap.

Существуют следующие различия между honeypot и проектом Honeynet.

- Honeynet — это не отдельная система, а целая сеть. Она находится за брандмауэром, где содержатся, записываются и контролируются все входящие и выходящие данные. Затем собранная информация анализируется для получения сведений о напавшем противнике. В пределах Honeynet можно разместить любую ОС и использовать в качестве honeypot, например Solaris, Linux, Windows NT, маршрутизатор Cicso и т.д. Это создает сетевое окружение с более реалистичной для нападающего атмосферой. Кроме того, применяя различные системы с разными сервисами, такие как Linux DNS, Web-сервер Windows NT или сервер Solaris, можно узнать об огромном разнообразии многочисленных инструментов и тактических приемов blackhat.
- Все системы, находящиеся в Honeynet, — это реальные стандартные системы и приложения, точно такие же, какие можно найти в Интернет. Ничего не предпринимается для того, чтобы ослабить защиту систем. Используя их, можно узнать очень многое. Использование производственных систем в Honeynet делает ее уникальной. Ничто не имитируется, позволяя использовать точно такие же приложения и системы, отражающие все качественные характеристики, присущие внутренней сети. Риски и уязвимые места, раскрытые в пределах Honeynet, существенно помогают повысить безопасность внутренней сети.

3.2. Назначение Honeynet

Традиционно при обеспечении информационной безопасности придерживались оборонительной стратегии. Брандмауэры, системы обнаружения вторжения, шифрование — все эти механизмы используются как оборонительные средства для защиты чьих-то ресурсов. Стратегия заключается в том, чтобы как можно лучше защитить организацию, обнаружить прорывы в обороне, а затем прореагировать на них. Недостаток такого подхода в том, что он абсолютно оборонительный — нападает враг. Honeynet предназначена для изменения ситуации, таким образом, чтобы инициатива принадлежала организациям. Основная цель создания Honeynet заключается в сборе информации о враге. То есть специалисты организации смогут остановить нападение или прорыв обороны до того, как это произойдет. Обеспечение информационной безопасности часто сравнивается с военными действиями, такими как оборона крепости или партизанская война, а это значит, что организации могут стать хозяевами положения, изучив врага до того, как он нанесет удар.

Honeynet также предоставляет организации информацию о рисках и слабых местах в плане обеспечения безопасности, так как может состоять из тех же самых ОС и приложений, которые используются в производственной среде. Также можно использовать системы, которые нужно протестировать, или рассмотреть вопрос об их применении. Зачастую риски могут быть пропущены в реальном окружении из-за перегрузки данными. Например, использование сети на предприятии связано с таким большим объемом деятельности, что трудно определить, какая деятельность злонамеренна, а какая является частью нормального повседневного сетевого трафика. Однако в контролируемом окружении Honeynet гораздо легче обнаружить подобные риски.

За последние годы Honeynet Project значительно расширил возможности определения, реагирования, восстановления и анализа систем, подвергшихся нападению. Обычно при анализе взломанной системы нельзя предположить, насколько верны его результаты; остается только строить догадки. Преимущество работы с анализируемой системой Honeynet заключается в том, что в наличии уже есть многие ответы, так как каждый пакет и комбинации клавиш, посланные в систему, были зафиксированы. Затем можно отнестись к взломанной системе, как к «задачке», проверяя на ней, насколько хорошо можно определить случившееся при помощи разнообразных техник исследования. Потом можно сравнить результаты с данными, записанными в Honeynet. Эту информацию также можно использовать для того, чтобы выяснить, не были ли взломаны другие системы производственной сети. После того как определены подписи (сигнатуры) взломщика и атаки, можно просмотреть окружение в поисках таких же сигнатур и обнаружить взломанные системы, о которых было не известно.

При изучении Honeynet и ее целей, возникает справедливый вопрос: является ли техника ее развертывания провокацией? Системы, намеренно созданные для взлома, можно рассматривать как попытку спровоцировать взломщиков на преступление [3]. Однако участники Honeynet Project глубоко уверены, что Honeynet не является какой-то формой провокации по следующим причинам:

- задача Honeynet состоит не в том, чтобы поймать хакеров, а в том, чтобы научиться у них. Действия в пределах Honeynet записываются и анализируются, но не используются для возбуждения уголовных дел. В определенных случаях судебные органы извещались о сделанных находках. Однако эта информация не используется для возбуждения дел против конкретных лиц;
- системы в Honeynet практически не отличаются от многих других производственных сред. Единственное отличие заключается в том, что входящие и исходящие из Honeynet данные изучаются более пристально. Если рассматривать Honeynet как вид провокации, тогда под это определение попадают и многие производственные сети, находящиеся в Интернет;
- участники проекта Honeynet ничего не делают для того, чтобы привлечь внимание взломщиков к своим машинам. Их существование не рекламируется и люди не заманиваются с целью получения к ним доступа. Взломщики активно находят и нападают на эти системы по собственной инициативе.

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 blackhat, но и определить риски и слабости, существующие во внутренней среде. Основная ценность проекта Honeynet заключается именно в возможности обучения.

4. Как работает Honeynet

Одной из самых больших проблем при обнаружении и фиксации подозрительных действий, с которыми сталкиваются администраторы и приложения, обеспечивающие безопасность (такие как системы обнаружения атак) является перегрузка данных. В таком огромном количестве информации очень трудно определить, что относится к производственному трафику, а что — к подозрительным и «ненормальным» действиям. Администраторам ежедневно приходится просматривать сотни мегабайт журналов регистрации системы и брандмауэра. Производственный трафик постоянно изменяется и развивается, усложняя задачу определения «нормального» трафика. Сетевые системы обнаружения атак также постоянно сталкиваются с необходимостью каким-то образом исключать ошибочные результаты, когда высылается предупреждение о подозрительных действиях при отсутствии таковых. Honeynet решает эту и многие другие проблемы благодаря своей простоте.

Идея такова — создать жестко контролируемую сеть. В пределах этой сети разместить производственные системы, а затем выполнять наблюдение, запись и анализ всех действий, происходящих в ней. Так как это не производственная система, а все-таки Honeynet, весь трафик является *изначально подозрительным*. Если кто-то инициирует соединение с системой, входящей в Honeynet, это, скорее всего, означает проведение какого-то сканирования или зондирования системы или сети. Если система, входящая в Honeynet, инициирует исходящее соединение, значит, она была взломана. Это упрощает весь процесс исследования, так как записывается совсем немного данных. По умолчанию вся собранная информация подозрительна. Затем можно легко и быстро сконцентрироваться на той информации, которая имеет наибольшую ценность.

Создание и поддержка Honeynet зависит от двух важных составляющих — контроля и записи данных [3]:

— 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 blackhat 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*.

4.1. Контроль данных

Контроль данных — это учет входящей и исходящей информации. Администратор решает и проверяет, какие данные могут идти по определенному адресу. Эта функция имеет огромное значение. После того как система, входящая в Honeynet, будет взломана, администратор несет ответственность за то, чтобы ею не воспользовались для нападения на производственные системы в других сетях. На рисунке 1 изображена примерная Honeynet, в том числе структура для контроля

данных. Ключевым элементом контроля данных является устройство проверки трафика, такое как брандмауэр. Он используется для того, чтобы отделить Honeynet от производственных сетей или от остальной части сети Интернет. Любые данные, входящие или исходящие из Honeynet, обязательно должны сначала пройти через брандмауэр.

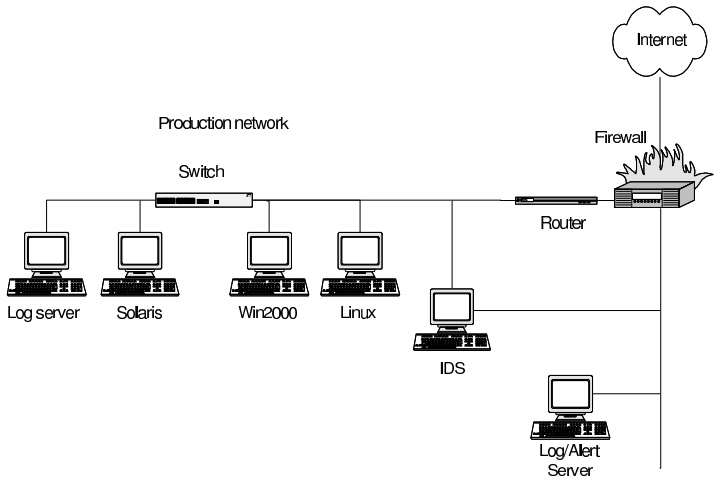

Рис. 1. Пример структуры сети Honeynet

Брандмауэр отслеживает поток трафика, функционируя по следующим правилам:

1. Любой желающий может инициировать соединение с Honeynet из Интернет, что позволяет взломщиками сканировать, зондировать и, в конечном счете, взламывать системы, входящие в Honeynet.
2. Брандмауэр контролирует то, как honeypot инициирует соединение с Интернет, то есть не позволяет blackhat воспользоваться Honeynet для нападения или взлома других производственных систем в доверенных сетях.
3. Honeynet и административная сеть не имеют каналов прямого сообщения, что гарантирует невозможность изменения или разрушения собранной информации.

После того как honeypot подвергнется нападению, необходимо сдержать действия взломщика, то есть установление blackhat соединений, исходящих из Honeynet. Объем разрешаемых действий зависит от уровня приемлемого риска. Чем больше действий разрешается, тем больше риск и тем больше можно узнать. После того как honeypot оказывается взломанной, хакеры, скорее всего, установят соединения с Интернет, преследуя различные цели: украсть инструментарий, установить соединение *IRC (Internet Relay Chat)*, просканировать другие системы и т.д. Однако эти действия необходимо контролировать. Если их не сдержать каким-либо способом, то риск будет очень высок. Именно здесь вступает в силу брандмауэр, призванный минимизировать риск.

Некоторые пользователи могут запретить все исходящие соединения с Интернет, так как это сводит практически весь риск к минимуму. Однако это, скорее всего, не сработает. После компрометации honeypot большинство взломщиков заподозрит неладное, если они не смогут установить ни одного соединения с Интернет. Атакованная honeypot может потерять ценность для взломщика, который хотел установить исходящие соединения. Когда honeypot не представляет особой ценности, то взломщик, вероятно, покинет систему и что-то узнать будет маловероятно. Необходимо разрешить определенное число исходящих соединений, но не слишком большое, чтобы не подвергать риску другие системы. Все зависит от того, что необходимо узнать и степени готовности рисковать.

Участники проекта Honeynet установили, что лучше всего разрешить от пяти до десяти соединений за сутки [8]. Нарушители получат достаточную степень маневренности, чтобы завершить те действия, которые они намеревались совершить. Однако, это не позволяет установить достаточно соединений для того, чтобы произвести атаку типа отказ в обслуживании, системное зондирование или какие-то иные злонамеренные действия. Необходимо помнить, что взломщик может прозондировать и атаковать другие системы в локальной сети Honeynet. На самом деле это было бы идеально, если бы так и произошло. По мере того как взломщики нападают на различные системы в пределах самой Honeynet, количество важной информации только растет. Однако основная задача заключается в том, чтобы сдержать трафик, идущий из Honeynet по направлению к Интернет или другим доверяемым сетям.

Очень важно точно настроить программу, направленную против получения доступа путем подмены IP *(IP-spoofing)*. Программы защиты от поддельных адресов гарантируют, что из сети Honeynet будут выходить только санкционированные пакеты. Проблема этого решения заключается в том, что взломщики обнаруживают, как брандмауэр фильтрует их трафик, а задача Honeynet может считаться успешно выполненной, только если взломщики не догадываются, что они находятся в системе honeypot. Необходимо внедрить какой-то метод сокрытия брандмауэра. Один из успешно применяемых способов заключается в размещении маршрутизатора между брандмауэром и Honeynet. При этом достигается несколько целей. Во-первых, маршрутизатор экранирует Honeynet от брандмауэра. После того как honeypot оказывается взломанной, нарушители видят вместо брандмауэра стандартный маршрутизатор. В большинстве случаев они ожидают увидеть именно его. Во-вторых, маршрутизатор можно использовать для контроля за правильностью IP-адресов. Применив выходной фильтр, можно быть уверенным, что через маршрутизатор пройдут только правомочные пакеты. Наконец, маршрутизатор можно использовать как дополнительное средство регистрации.

Теперь, когда осуществлен контроль за потоком данных, следующая задача заключается в записи информации.

4.2. Запись данных

Запись данных — это фиксация всех действий, происходящих в пределах Honeynet, в том числе на уровне системы и сети. Именно в этом и заключается цель Honeynet, а точнее — в записи и изучении данных. Если не суметь записать данные, потеряет значение весь проект. Что толку обнаружить «элитарный» взлом системы honeypot, если можно потерять или нельзя зафиксировать информацию? Правильная запись данных крайне важна для успеха всего проекта. Ключом к успеху является большое количество разных способов записи информации: чем больше их, тем лучше. Не нужно зависеть от единственного способа. Кроме того, записывая информацию несколькими способами, можно составить на ее основе более полную картину того, какие инструменты и тактику применил взломщик, а также его мотивы.

Сначала нужно хорошо запомнить, что никакие собранные данные не могут храниться в локальных системах Honeynet. Любая собранная информация должна храниться в защищенной системе, к которой у взломщика нет доступа. Этот момент очень важен по причине обнаружения и потери данных:

- если данные, например история клавиш, использованных взломщиком, сохранена в локальной системе, то эта информация может быть обнаружена и потенциально использована для взлома honeypot и разрушения системы;
- взломщик может изменить или стереть хранящиеся в локальной системе данные. Например, стереть жесткий диск после того, как воспользуется системой. Если взломщик обнаружит, что данные записываются, он может их уничтожить, или, что еще хуже, изменить, предоставив вам ложную информацию.

4.2.1. Уровень контроля доступа

Первый уровень контроля доступа состоит из устройств контроля доступа, таких как брандмауэр и маршрутизатор. Любой пакет, входящий или исходящий из Honeynet, должен пройти через эти устройства, вот почему они являются превосходным источником информации. Многие пользователи считают журналы регистрации брандмауэра бесполезными, так как ежедневно там записывается по 100-500 Мб данных. Объем этой информации может показаться очень большим, и его трудно анализировать. Однако необходимо помнить, что любые данные, входящие или исходящие из Honeynet, подозрительны.

Объем трафика, который является сомнительным, просто поражает. То, что кажется ложным сообщением об ошибке ICMP, может означать, что кто-то сканирует системы в поисках черного хода. То, что кажется ошибочной попыткой установления соединения telnet, на самом деле означает, что кто-то сканирует систему в поисках троянских логинов, которые ищут настройку терминала ELITE. Важно не только зарегистрировать эту информацию на брандмауэре, но и получить сообщение о ней. Брандмауэр Honeynet нужно настроить так, чтобы он предупреждал администраторов всякий раз, когда предпринимается попытка установить исходящее соединение.

4.2.2. Сетевой уровень

Второй, сетевой, уровень сбора данных состоит из записи и анализа всех пакетов, путешествующих в сети. На этом уровне собирается информация двух видов: предупреждения о подозрительных сигнатурах и полезная нагрузка пакетов. Как правило, эти две функциональных особенности сочетаются с системой обнаружения атак, так как большинство подобных систем могут и записывать всю полезную нагрузку пакетов, и высылать предупреждения на основании подозрительных сигнатур. Команда Honeynet Project успешно работает с IDS Snort — бесплатной открытой IDS (`http://www.snort.org`). Забавно, но важными оказались не возможности предупреждения IDS, а возможность записи данных. Важно помнить, что основная задача IDS заключается в том, чтобы определить подозрительные действия и предупредить о них. По определению, любые действия по отношению к Honeynet или исходящие из нее подозрительны, так что процесс предупреждения становится простым. Что действительно важно, так это возможность записывать пакеты в простом для анализа формате. Следовательно, необходимо настроить IDS, в данном случае Snort, так, чтобы записывать и хранить данные в трех форматах.

1. Во-первых, нужно настроить Snort так, чтобы она оповещала о любом подозрительном поведении (что является традиционной задачей системы обнаружения вторжения). Эти предупреждения посылаются через программу syslogd на сервер регистрации в административной сети. Предупреждения хранятся, например, в централизованном системном журнале (`/var/log/messages`), за которым постоянно наблюдает программа Swatch [9].
2. Во-вторых, Snort записывает каждый пакет, исходящий из сети, и его полную полезную нагрузку, после чего сохраняет эти данные в двоичном формате. Затем собранные данные используются для дальнейшего анализа.
3. Также можно сконфигурировать Snort, чтобы она конвертировала любую информацию в формате ASCII, найденную в пакетах, в легкий для чтения однородный файл, который называется *врезкой сеанса связи* (session breakout). Это великолепно подходит для быстрого анализа сеансов связи с открытым текстом, таких как FTP, telnet или IRC.

Перехватчик пакетов (sniffer) можно разместить в любом из нескольких мест. Например, на брандмауэре. Так как все данные проходят через брандмауэр, то он представляет собой отличное место для записи потоков информации. Однако запуск такого приложения может подвергнуть брандмауэр риску. Тот, кто может взломать программу записи пакетов, сумеет взломать и брандмауэр, так как они функционируют в одной и той же системе. При наличии ресурсов более безопасное

решение — создание специализированной IDS, которая может записывать весь трафик сети. Очень важно, чтобы записывался весь трафик: как входящий/исходящий из Honeynet, так и потоки между системами honeypot в пределах Honeynet. После того как honeypot будет взломана, нарушитель наверняка попытается напасть и на другие системы, входящие в Honeynet. Эта информация также должна фиксироваться. Вот еще одна причина для создания специализированной IDS, поскольку ни брандмауэр, ни системы контроля доступа записать эти данные не смогут.

4.2.3. Системный уровень

При записи всех данных нельзя зависеть от регистрационных журналов брандмауэра или модулей проверки текущего состояния. Например, если взломщик использует при работе с Honeynet шифрование данных, в частности ssh, запись их усложняется, так как сетевые данные зашифрованы. Необходимо записывать комбинации клавиш и действия в системе внутри программ, например в ssh.

Для сбора данных и удаленного их хранения существует несколько методов. Первый метод заключается в использовании выделенного сервера syslog во внутренней сети Honeynet. Задача syslog состоит в сборе всех системных журналов Honeynet. Системные журналы — это отличный источник информации, поскольку они обычно регистрируют то, как хакер взломал систему и получил к ней доступ. Тем не менее после атаки взломщики зачастую изменяют или стирают именно системные журналы. По этой причине нужно хранить информацию удаленно на защищенном сервере.

Сервер syslog также служит еще одной, более коварной задаче. Сервер syslog представляет собой сложную систему honeypot и, следовательно, наиболее защищенную систему в Honeynet. На примере этой honeypot можно изучить наиболее изощренные инструменты и тактику сообщества blackhat. Когда они взламывают одну из менее защищенных систем Honeynet, то могут заметить, что system logs переправляются на удаленный сервер. Многие из атакующих попытаются взломать удаленный сервер, чтобы скрыть свои следы и уничтожить записи. Однако удаленный регистрационный сервер — гораздо более защищенная система, для взлома которой требуются изощренные инструменты и сложная тактика. Таким образом, можно узнать намного больше, если взломщик нацелится на регистрационный сервер. Необходимо иметь в виду, что, даже если будет взломан удаленный сервер syslog и все записи будут стерты, ничего не потеряется, так как сервер IDS, который записывает все пакеты, также фиксирует все регистрационные файлы, посылаемые на удаленный сервер syslog, потому что эта информация пересылается в пределах сети. IDS выступает в качестве вторичного, но пассивного сервера syslog. Таким образом, не только регистрационные файлы удаленно регистрируются на сервере syslog, но и все system logs пассивно записываются в IDS. Очень важно помнить, что многоуровневая запись данных имеет огромное значение.

4.2.4. Автономный уровень

После взлома составляющие элементы сети Honeynet могут предоставить огромное количество информации. Для этого, как правило, требуется перевести системы в автономный режим или сделать их зарисовки. Системы могут располагать обширными данными, в том числе об использованных взломщиком инструментах, исходном коде, словаре паролей, файлах конфигурации и системных файлах, таких как `.history`. Перед созданием системы и ее запуском необходимо выполнить некоторые действия. Например, воспользоваться утилитой Tripwire, с помощью которой можно сделать снимок системы honeypot перед тем, как размещать ее в сети Honeynet.

Когда через какое-то время система будет взломана, можно будет воспользоваться базой данных Tripwire, чтобы определить измененные бинарные файлы или файлы конфигурации системы. Создавая снимки взломанной системы, можно проводить ее автономный анализ, чтобы определить, что именно сделал взломщик.

Можно восстановить действия blackhat, даже не зная комбинаций клавиш. Также можно восстановить инструментарий и код, использованный взломщиком, даже если они были удалены.

5. Тактика, инструменты и мотивы blackhat

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 blackhat, можно лучше узнать своего врага и лучше понять возникшую угрозу [8, 10].

5.1. Угроза

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. Нападающий выполняет свою задачу, выбирая для себя небольшое количество эксплойтов (специальные программные средства для взлома систем через определенные уязвимости), после чего ищет в сети Интернет нужные ему уязвимости, чтобы применить имеющиеся эксплойты, и рано или поздно жертва находится [5, 8].

Одни взломщики являются продвинутыми пользователями, которые разрабатывают собственные инструменты и оставляют за собой сложные черные ходы *(backdoor)*. Другие не имеют представления о том, что они делают; только знают, как набрать в командной строке *setup*. Независимо от уровня навыков все взломщики действуют по сходной стратегии: случайным образом ищут слабые места системы, а затем пользуются ими. Именно случайный выбор целей и превращает эту стратегию в такую серьезную угрозу. Все системы и сети будут неизбежно прозондированы, скрыться невозможно. Многие администраторы бывают поражены тем, что их системы были просканированы в течение всего двух дней после подключения к сети, когда никто о них не знал. Здесь нет ничего удивительного. Скорее всего, системы были просканированы взломщиком, который как раз «прочищал» этот блок IP-адресов.

Если бы эта техника ограничивалась несколькими отдельными случаями сканирования, статистика была бы более обнадеживающей. Так как в Интернет находятся миллионы систем, шансы, что кто-то найдет кокнкретную систему, крайне малы. Однако это не тот случай. Большинство подобных инструментов просты в применении и широко распространены — любой желающий может ими воспользоваться. Когда огромное число пользователей Интернет применяет эти инструменты, вопрос состоит уже не в том, будет ли прозондирована конкретная система, а в том, когда это произойдет. Если система была подключена к Интернет более 24 часов назад, возможно, ее уже прозондировали.

5.2. Тактика

За прошедшие несколько лет команда Honeynet Project от случая к случаю наблюдала применение против Honeynet одной и той же тактики. Хотя не все взломщики прибегают к этой тактике, она относится к наиболее распространенным способам действия. Она очень проста. Большинство взломщиков случайным образом сканируют Интернет в поисках определенных уязвимых мест, чтобы впоследствии их использовать. Большинство применяемых инструментов просты в использовании и автоматизированы, так что не требуют особого взаимодействия с пользователем. Можно запустить инструмент и вернуться через несколько дней, чтобы просмотреть результаты. У взломщиков есть даже название для этого вида инструментов — autorooter [4, 11]. Ни один инструмент не похож на другой, точно

так же, как не бывает двух одинаковых взломов. Однако большинство инструментов основывается на одной и той же тактике. Сначала взломщик создает базу данных IP-адресов, которые можно просканировать. Следующий этап заключается в сборе информации об этих IP-адресах: какая используется ОС и какие сервисы или приложения предлагаются. Зачастую необходимо определить версию сервиса или приложения. После того как будет получена эта информация, сам взломщик или его инструмент определяет, насколько уязвима удаленная система. Однако в последнее время хакеры даже не утруждают себя определением уязвимости системы. Они запускают свои приемы против множества систем и смотрят, насколько успешной была попытка.

Не все blackhat абсолютно точно следуют этой тактике. Например, многие взломщики не утруждают себя созданием базы данных IP-адресов и просто последовательно сканируют всю сеть в поисках определенного сервиса. Если взломщик найдет требуемую систему, он не удосужится определить версию или поставщика работающего сервера, а просто начнет взлом. Если получится, хорошо. Если нет, он перейдет к следующей системе. Взломщики могут запустить процесс сканирования на 24 часа в сутки, 7 дней в неделю.

Можно подумать, что все это сканирование будет необычайно шумным и привлечет большое внимание. Однако многие пользователи не проводят мониторинг своих систем и не понимают, что их сканируют или что их системы используются для сканирования других систем. Кроме того, многие script kiddies спокойно ищут одну систему, которую могут взломать. После этого ее используют в качестве стартовой площадки, напрямую сканируя весь Интернет, не опасаясь наказания. Если такие попытки будут обнаружены, отвечать придется системному администратору, а не взломщикам.

После проведения атаки более опытные взломщики устанавливают троянские программы или черные ходы, которые позволяют получить быстрый и незаметный доступ к системе. Даже если администратор изменит учетные записи или пароли, у взломщика все равно будет удаленный доступ. В системные двоичные файлы внедряются троянские программы, скрывающие присутствие и действия взломщиков. Троянцы делают незваного гостя незаметным, не запоминая его действия ни в системных журналах, ни в процессах, ни в структуре файлов. Более сложные троянцы модифицируют системные библиотеки или даже загружают узловые модули, изменяя работающее в памяти ядро. Для автоматизации и упрощения этой задачи были созданы и опубликованы инструменты под названием rootkit [11,12]. Они автоматизируют весь процесс подчинения себе системы, включая зачистку системных журналов для сокрытия следов действия взломщика, замену системных двоичных файлов, установку черного хода и запуск анализаторов для перехвата учетных записей и паролей. Участникам Honeynet Project даже встречались rootkit, охранявшие скомпрометированную систему, чтобы никакой другой взломщик не мог найти и воспользоваться тем же самым уязвимым местом.

5.3. Инструменты

Используемые инструменты 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. Лишь небольшой процент взломщиков владеет такой информацией. Разработка инструментов для взлома не относится к прерогативе взломщиков; во многие корпоративные продукты вносятся изменения, после чего они используются в корыстных целях. Однако инструменты разрабатываются или изменяются таким образом, чтобы любой желающий мог ими воспользоваться, имея смутное (или не имея вообще) представление о принципе их работы. В результате все большее число хакеров получает доступ к мощным инструментам, которые сложны для разработки, но необычайно просты в использовании. Большинство инструментов предназначается только для одной задачи с малым количеством опций, частично потому, что запрограммировать и использовать простые функции легче и быстрее. Однако функциональные возможности некоторых инструментов начинают возрастать, так

что вместо того, чтобы запускать пять программ ради выполнения одной задачи, можно запустить только одну.

Стоит сказать об инструментах, используемых при создании базы данных IP-адресов. Эти инструменты действуют случайным образом, так как сканируют все системы в Интернет. Например, многие инструменты имеют только одну опцию: A, B или C. Выбранная буква обозначает класс сети, которая будет просканирована. Затем эти инструменты случайным образом выбирают, какую область IP-адресов сканировать. Другие инструменты пользуются именем домена (например, zOne) и создают базу данных IP-адресов путем проведения сканирования зоны доменного имени и всех поддоменов. Путем сканирования целого домена `.com` или `.edu`, взломщики создали базы данных, содержащие более 2 миллионов IP-адресов. После обнаружения эти адреса сканируются при помощи специальных инструментов с целью определения уязвимых мест, таких как версия ОС или запускаемые в системе сервисы. Зачастую эти инструменты сначала ищут определенный сервис, а затем определяют его версию. После того как уязвимые системы определены, взломщик наносит удар.

Для автоматизации всего этого процесса также были разработаны особые инструменты. Этапы сканирования, определения и атаки на системы встроены в один пакет программ. После запуска эти автоматизированные инструменты часами выполняют задания взломщиков.

Например, одна из honeypot Honeynet Project с системой UNIX была взломана через rpc.statd, затем злоумышленники попытались воспользоваться ею как платформой для сканирования и взлома других систем в Интернет. С этой целью был выбран autorooter — инструмент, автоматически выполняющий весь процесс путем последовательного сканирования, зондирования и взлома тысячи систем [4]. Этот инструмент даже автоматизировал процесс загрузки и инсталляции rootkit, обеспечивая принадлежность к взломанной системе. В течение четырех часов было зарегистрировано более чем 500 000 попыток просканировать системы. Все попытки были заблокированы; однако их число говорит о том, как агрессивно и совершенно случайно могут работать подобные инструменты.

5.4. Мотивы

Мотивы взлома случайных уязвимых систем разнообразны. Каждый раз при взломе honeypot информация об использованных инструментах и тактике, а также почему было совершено нападение оказывается наиболее интересной и полезной.

Одним из мотивов может быть проведение атаки типа отказ в обслуживании. В последнее время распространение получают атаки на отказ в обслуживании нового вида: *DDoS (Distributed Denial of Service — распределенная атака на отказ в обслуживании)*. При проведении таких атак одна blackhat управляет сотнями, если не тысячами, взломанных систем по всему миру. Действия взломанных систем подчиняются удаленному координированию для проведения атаки типа отказ в обслуживании на одну или несколько жертв. Так как в атаке участвует множество взломанных систем, невероятно трудно защититься и определить источник нападения. Для того чтобы такая атака удалась, взломщику необходим доступ к сотням взломанных систем. Чем больше скомпрометировано систем, тем мощнее нападение DDoS.

Также нужно сказать о желании взломщиков скрыть свой исходный код и идентификацию [6]. При нападении на определенную систему взломщики не хотят, чтобы следы привели прямо к ним. Они могут замаскировать свои истинные данные, если будут взламывать систему из цепи уже взломанных систем. Вместо того, чтобы напрямую нападать на систему из места собственного расположения, они взламывают системы через несколько прыжков (смен IP-адреса). Это невероятно усложняет задачу выслеживания взломщика, так как необходимо пройти через ряд взломанных систем. Скорее всего, где-нибудь посередине пути взломщик полностью сотрет все следы. Для того чтобы еще больше затруднить выслеживание, атакующие могут взламывать системы в различных странах с разными временными поясами, языком и правительственной структурой. Администраторам и властям

очень трудно идти по следу нападения в таких условиях. Языковые барьеры, временные пояса и политические системы могут вообще превратить выслеживание цепи взломанных систем в невыполнимую задачу.

Еще одним мотивом для случайного взлома систем является IRC. Зачастую взломщики хотят иметь на своем IRC канале права администратора (sys ops). Для того чтобы удерживать эти права, взломщику нужно поддерживать присутствие на канале. Автоматизированный инструмент, bot, позволяет этого добиться. Обычная тактика заключается в том, чтобы взломать как можно больше систем и запустить на них боты. Чем больше взломано систем, тем больше ботов у взломщика. Чем больше их у взломщика, тем большей властью он пользуется на каналах IRC. Эти же системы можно использовать для проведения нападений отказ в обслуживании против других взломщиков, чтобы уничтожить их боты и, тем самым, закрыть им доступ в каналы IRC.

Кроме того, такие каналы являются основным средством общения среди взломщиков. В рамках Honeynet Project неоднократно были взломаны honeypot с целью поддержания такого сообщения. В одном случае был установлен не только бот, но и BNC — утилита, позволяющая устанавливать через систему proxy-соединения.

Еще один мотив — возможность похвастаться. Многие blackhat любят бахвалиться тем, сколько систем они взломали. Неважно, какие это были системы, главное, чтобы их было больше, чем у остальных коллег. Зачастую нарушители рекламируют свои действия тем, что взламывают Web-сайты, а затем меняют их содержимое (например, первую страницу). Взломанные сайты также можно использовать как центры хранения и распространения информации. Нарушители часто настраивают Web-сайты на распространение инструментов, документов, взломанного ПО, музыки, фотографий и других файлов [8].

Таким образом, мотивы нападения так же разнообразны, как и сами взломщики. Нет одного, общего для всех, мотива. Зачастую взломщики пытаются оправдать свои действия, заявляя, что они политически оправданы, например, в качестве возмездия несправедливой политической системе или конкретным корпорациям. Нарушители часто оставляют сообщения о мотивах своих действий. Однако эти оправдания, в основном, всего-навсего воображаемые причины, прикрываясь которыми, взломщики пытаются удовлетворить собственные желания.

5.5. Меняющиеся тенденции

За прошедшие несколько лет замечено несколько изменений в инструментах и тактике взломщиков. Эти изменения указывают на возрастающую угрозу безопасности. Среди самых значительных перемен можно выделить четыре, касающихся тактики сканирования, использования шифрования, сложных rootkit и червей [8].

Тактика сканирования становится все более агрессивной. Обычно перед началом нападения взломщикам требовалось время на то, чтобы определить системы, уязвимые для действий конкретного вида. Однако сейчас взломщики не утруждают себя вычислением подобных систем — они просто определяют сервис и пытаются взломать его независимо от типа ОС или версии. Например, Honeynet Project поддерживает инсталляции по умолчанию систем Linux и Solaris, в каждой из которых запущен сервис `rpc.statd`. В среднем эти системы сканировались от одного до трех раз в день, зачастую для определения RPC. Затем взломщики просто запускали свой сценарий атаки. Однако тот же самый сценарий запускался и для системы Intel Linux, и для системы SPARC Solaris, несмотря на то, что этот прием действует только против Linux.

В течение января 2001 года было совершено 19 атак типа rpc.statd на систему honeypot Solaris, хотя она не уязвима для подобного нападения. Это указывает на то, что взломщики не тратили время на точное определение уязвимых систем. Если у blackhat есть сомнения, они просто запускают свой сценарий и переходят к следующей системе. Подобная агрессивная тактика может потенциально нанести вред, разрушив сервисы или даже систему. В некоторых организациях, например, меняют номер версии приложения, чтобы незащищенное приложение казалось надежным. Более того, изменяют и приложение, чтобы оно не выдавало номер своей

версии. Те специалисты, которые полагают, что этими методами они защищают себя, сильно заблуждаются. Необходимо иметь в виду, что взломщики зачастую даже не утруждают себя определением версии — они просто нападают на систему и переходят к следующей. Команда Honeynet Project раз за разом наблюдала применение этой тактики.

Вторая тенденция — шифрование — затрудняет выслеживание взломщиков. Обычно Honeynet Project фиксирует действия взломщиков, записывая их команды и анализируя деятельность в сети. Однако этот метод не надежен, так как для работы со взломанными системами используется шифрование. Многие ОС, такие как Linux или OpenBSD, укомплектованы программой ssh. После проведения атаки взломщики для управления системой вместо telnet пользуются ssh, которая кодирует весь трафик взломщика, защищая его, тем самым, от систем обнаружения вторжения или от анализа сети. Даже если утилиты шифрования не установлены, взломщики могут установить свои собственные. В пяти последних нападениях на системы honeypot проекта взломщики загружали и инсталлировали собственные утилиты шифрования, чтобы защитить себя от мониторинга своих действий. Во всех случаях были использованы троянские версии ssh, которые не только шифруют действия, но и устанавливают в системе черный ход. Таким образом, кодирование значительно затрудняет отслеживание взломщиков. В свою очередь, участники проекта наблюдали за действиями blackhat на системном уровне, например, за установкой троянских оболочек или драйверов в ядре, которые фиксируют команды и передают эти данные в доверенную систему.

Третье изменение, которое наблюдала команда Honeynet Project, заключается в использовании более совершенных rootkit. Традиционные rootkit замещали системные бинарные файлы, скрывая действия взломщиков и устанавливая черные ходы. Современные rootkit способны вносить изменения в ядро ОС (например, Adore). Например, если выполнить команды `ls` или `find`, то результату их выполнения нельзя доверять, поскольку нельзя доверять ядру. Поэтому после взлома системы задача отслеживания нарушителей становится более сложной. В отношении этих rootkit на уровне ядра особенно важно, что двоичные файлы в системе не изменяются. В случае с традиционными rootkit нападающий модифицирует двоичные файлы, в частности `ls` или `whois`, а это означает, что такие программы, как Tripwire, могут определить, изменялся ли файл. Однако сейчас модифицируется само ядро, двоичные файлы не изменяются, следовательно, программы типа Tripwire больше не могут определить установленный rootkit. Такие rootkit на уровне ядра обладают большими возможностями и их очень трудно обнаружить.

Четвертая тенденция кажется наиболее угрожающей. Взломщики создали червей, которые не только автоматизируют зондирование и нападение, но также создают собственные копии. Это означает, что количество взломанных систем может возрастать по экспоненте, с малым числом или вовсе без участия взломщиков. После взлома системы червь использует ее как базу для своего воспроизведения, сканируя и взламывая другие системы. Он продолжает этот процесс, получая контроль над большим количеством систем. Обычно поле деятельности червей ограничивалось системами на базе Windows. Однако в начале 2001 года команда проекта стала свидетелем возрастающего количества червей, таких как Ramen, Lion или Sadmind/IIS, нападающих на системы UNIX [8]. Эти черви ориентированы на те же инструменты и слабые места, о которых уже было сказано выше. Они очень опасны именно тем, что воспроизводят сами себя.

6. Honeypot в борьбе со спамом

Люди занимаются рассылкой спама не ради удовольствия, а потому, что за это платят деньги. Работу спамеров можно разделит на три стадии:

— сбор информации: построение базы данных электронных адресов реальных людей;
— невидимая работа через прокси: анонимная работа по рассылке электронных писем;

— рассылка спама: поиск и использование почтовых серверов, которые позволяют посылать письма с любым содержанием.

В этом параграфе будет показано, можно ли использовать технологию honeypot в следующих случаях:

— когда спамер берет e-mail с вашего web-сайта для дальнейшего внесения в базу данных;
— когда спамер использует прокси-сервер для доступа к какому-либо ресурсу;
— когда спамер пытается переслать трафик SMTP через ваш почтовый сервер для рассылки спама.

6.1. Honeypot и сбор адресов электронной почты

Одной из первых фаз в работе спамера является сбор адресов электронной почты. Вообще, кроме обмана спамеров с помощью honeypot, существует еще несколько эффективных способов, которые, тем не менее, не подходят под классическое определение honeypot. Концепция заключается в следующем: размещение на web-сайтах несуществующих адресов. Следовательно, когда спамеры просматривают web-страницы, они считывают оттуда фальшивые адреса и заполняют ими свою базу данных, что приводит к сильному увеличению самой базы и уменьшению процента реальных адресов, в ней содержащихся. Вообще-то, это не совсем honeypot, но по смыслу похоже.

Иногда, в процессе сбора реальных адресов по web, спамеров могут узнать из-за программ, которыми они пользуются для считывания поля User-Agent. Некоторые люди блокируют User-Agent, про который известно, что он используется спамерами; или прозрачно перенаправляют клиентов на специально созданные web-страницы, содержащие огромное количество несуществующих адресов. Вроде бы все просто, но проблема заключается в том, что спамеру совершенно не трудно изменить User-Agent. Поэтому люди, борющиеся со спамом, приняли решение создать гиперссылки, невидимые для посетителя сайта (например, белые буквы на белом фоне), но видимые программе, называемой spambot, которая переходит по любой ссылке, встречающейся в HTML-коде. Такая web-страница динамически создаст ложные адреса электронной почты, чтобы обмануть спамеров.

6.2. Honeypot и прокси-серверы

В большинстве случаев спамеры используют открытые прокси-серверы для рассылки писем. В этом случае, прокси выполняют роль стены, за которой прячутся спамеры. В этом случае можно подделать открытый прокси-сервер с помощью honeypot.

Если посмотреть на записи событий брэндмауэра, то можно заметить попытки получения доступа к TCP портам:

— 1080 socks прокси-сервер;
— 3128 squid прокси-сервер;
— 8080 web-кэширование.

Необходимо попробовать настроить несколько honeypot, которые будут отвечать на поступающие запросы. Так можно обмануть некоторых спамеров. Доказательством правильности концепции служит программа под названием Bubblegum Proxypot. Единственное, что умеет делать эта небольшая программка — это симулировать открытые прокси-серверы.

В Proxypot можно выбрать три различные конфигурации для обмана спамеров:

— smtp1: подделка всего SMTP соединения, от начала и до конца;
— smtp2: подключение производится к реальному SMTP серверу, идет считывание 220 баннера и, возможно, выполнение команды HELP, чтобы узнать тип этого сервера, потом отключение и использование этой информации для установления более убедительной симуляции соединения;
— smtp3: подключение к реальному SMTP серверу и выполнение всех команд, кроме DATA и EXPN.

Используя поддельные прокси-сервера, можно добиться замедления работы спамеров (путем замедления сетевых диалогов) и блокирования их действий (путем симуляции и препятствования отсылки спама), что помогает в нахождении спамеров.

6.3. Honeypot и открытый relay

Известно, что спамеры стараются найти открытые relay, чтобы отправлять груды писем без аутентификации. Подделать такой почтовый сервер совсем не сложно.

Интересное решение этой проблемы предложил Бред Спенсер: изменить неиспользуемый демон sendmail для обмана спамеров [13]. Это можно легко осуществить, заставив sendmail пропускать relay и помещать в очередь все письма, при этом не отправляя ни одного. Таким образом настроенный sendmail может блокировать все входящие письма.

Еще одно решение — демон Spamd, созданный командой OpenBSD. Spamd симулирует sendmail сервер, запрещающий поддельную почту. Его задачей является занять как можно больше времени и ресурсов спамера.

Конечно, Honeyd — еще одно простое решение для создания поддельных почтовых серверов, симулирующее relay.

6.4. Итоги

К концу октября 2003 была найдена новая программа для открытия черного хода Hogle (Proxy-Regate). Она заражала компьютеры с ОС Windows и устанавливала SMTP-прокси сервис, работающий на TCP порту 3355, который был использован спамерами. Этот пример далеко не единственный, и таких примеров становится все больше.

В начале ноября 2003 г. разные версии червя MiMail были запущены, и некоторые из них производили DoS атаки на web-серверы, которые были предназначены для борьбы со спамом. Эти черви атаковали сайты `spews.org`, `spamgaus.org` и `spamcop.net`.

Спамеры распространили червей по всему миру для контроля за миллионами хостов, и эти хосты могут быть использованы для спама в любой момент. Похоже, что будущее у пользователей Интернета весьма мрачное.

Honeypot вполне способна помочь в этой битве. Для этого необходимо развернуть новый тип honeypot — активных, которые будут способны симулировать инфицированный компьютер, делая вид, что он заражен и ждет удаленных команд. Это поможет понять новые методики и мотивации, используемые новым видом спамеров.

7. Заключение

Honeynet — специальное средство, предназначенное для сбора разведывательных данных об инструментальных средствах, тактике и мотивах сообщества blackhat. Оно включает в себя все положительные стороны honeypot, в частности работу в качестве ложной цели и системы оповещения, однако ее основное предназначение — изучение. Между honeypot и Honeynet есть два принципиальных различия. Первое различие состоит в том, что Honeynet не одиночная система, а сеть, состоящая из нескольких систем и приложений. Второе различие в том, что в состав Honeynet входят самые обычные системы, которые можно повсюду встретить в Internet; т.е. ничто не эмулируется — ни системы, ни уязвимости. Такая комбинация делает Honeynet превосходным средством для обучения. Однако Honeynet требует огромного количества административных затрат. Администратор Honeynet несет ответственность за то, чтобы другие системы не были атакованы с использованием скомпрометированной Honeynet. Без надлежащего администрирования риски могут превышать получаемую выгоду.

Honeynet не является панацеей в области безопасности и не является подходящим решением для каждой организации. Для решения проблем безопасности необходимо использовать зарекомендовавшие себя методы, такие как строгая аутентификация, использование протоколов с криптографической защитой, регулярный просмотр системных журналов и использование защищенных решений. Приоритет следует отдать четкой регламентации и описанию процедур, так как это поможет снизить риск. Honeynet может помочь лишь тогда, когда перечисленные выше меры защиты уже приняты, неукоснительно выполняются и сопровождаются и предпринимаются все стандартные меры обеспечения безопасности, типа своевременного внесения изменений в системы и отключения ненужных сервисов. Лишь после этого можно задуматься о построении и использовании Honeynet для сбора информации и изучения противника.

Литература

1. *Спитцнер Л.* Honeynet Project: ловушка для хакеров // Открытые системы. — № 7-8. — 2003. — http://www.osp.ru/os/2003/07-08/061.htm.
2. *Мяснянкин В.* Все любят мед // LAN. — № 4. — 2002. — http://www.osp.ru/lan/2002/04/084.htm.
3. *The Honeynet Project*. Know Your Enemy: Honeynets. Whitepaper. — 2003. — http://project.honeynet.org/papers/honeynet/index.html.
4. *The Honeynet Project*. Know Your Enemy: The Motives and Psychology of the Blackhat Community. Whitepaper. — 2000. — http://project.honeynet.org/papers/motives/index.html.
5. *The Honeynet Project*. Know Your Enemy: The Tools and Methodologies of the Script Kiddie. Whitepaper. — 2000. — http://project.honeynet.org/papers/enemy/index.html.
6. *The Honeynet Project*. Know Your Enemy: Learning About Security Threats. — second edition. — Addison-Wesley Professional, 2004. — 768 p.
7. *Oudot L.* Fighting Spammers With Honeypots. — 2003. — http://www.securityfocus.com/infocus/1747.
8. Инструменты, тактика и мотивы хакеров. Знай своего врага / под ред. И. М. Захаров. — М.: ДМК Пресс, 2003. — 312 с.
9. *The Honeynet Project*. Know Your Enemy: A Forensic Analysis. Whitepaper. — 2000. — http://project.honeynet.org/papers/forensics/index.html.
10. *The Honeynet Project*. Know Your Enemy II: Tracking the blackhat's moves. Whitepaper. — 2001. — http://project.honeynet.org/papers/enemy2/index.html.
11. *Spitzner L.* Honeypots: Tracking Hackers. — Addison-Wesley Professional, 2002. — 480 p.
12. *The Honeynet Project*. Know Your Enemy III: They Gain Root. Whitepaper. — 2000. — http://project.honeynet.org/papers/enemy3/index.html.
13. *Spencer B.* Fighting Relay Spam the Honeypot Way. — 2002. — http://www.tracking-hackers.com/solutions/sendmail.html.

UDC 004.056.53

Main Purposes of the Honeynet Project

D. S. Kulyabov, A. V. Ulianov

Telecommunication Systems Department
Peoples' Friendship University of Russia
Miklukho-Macklaya str., 6, Moscow, 117198, Russia

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 blackhat community based on the results of the Honeynet Project Organization.