ВВЕДЕНИЕ

Настоящее, третьей издание этой книги было написано и отредактировано в течение полутора лет, т.е. от конца 2015 года и до начала 2017 года, приблизительно через шесть лет после выхода в свет второго издания и десять лет после первого издания. В настоящее издание вошло немало нового, включая совершенно новые файлы и сценарии перехвата, а также отдельную новую главу, посвященную анализу пакетов из командной строки с помощью утилит TShark и `tcpdump`. Если вам понравились два предыдущих издания, то понравится и третье. Оно написано в том же духе с пояснениями простым и доходчивым языком. А если вы сомневались в выборе двух предыдущих изданий, поскольку они не содержали самые последние сведения об организации сетей и обновлениях Wireshark, в таком случае вам придется прочитать настоящее издание, которое было дополнено описанием новых сетевых протоколов и обновленной информацией по версии Wireshark 2.*x*.

Зачем нужна эта книга

У читателя может возникнуть вполне резонный вопрос: чем эта книга отличается от других книг на тему анализа пакетов? Ответ заключается в названии книги *Практика анализа пакетов*. Следует откровенно признать, что ничто не может сравниться с практическим опытом, и точнее всего этот опыт удается передать в книге на практических примерах и реальных сценариях.

В первой половине книги даются знания, необходимые для уяснения особенностей анализа пакетов и работы с Wireshark. А вторая ее половина полностью посвящена разбору случаев из повседневной практики управления сетями.

Усвоив методики анализа пакетов, описанные в этой книге, читатель извлечет для себя немалую пользу, кем бы он ни работал: сетевым техником, сетевым администратором, руководителем информационной службы, специалистом по настольным системам или даже аналитиком по вопросам безопасности сетей.

Основные понятия и принятый подход

Вообще-то, я нетороплив и когда поясняю какое-нибудь понятие, то стараюсь делать это непринужденно. Это же относится и к языку, которым изложен материал книги. Чтобы не увязнуть в техническом жаргоне, я попытался изложить описываемые в ней понятия как можно более простым и обыденным языком. Все термины и понятия определяются в ней без каких-либо несущественных подробностей. Ведь я родом из замечательного штата Кентукки, а следовательно, стараюсь быть немногословным. (Но вы, читатель, простите мне излишнюю многословность, которой я иногда грешу в книге.)

Первые несколько глав существенны для понимания остальной части книги, поэтому непременно усвойте описываемые в них понятия. А вторая половина книги всецело посвящена разбору практических примеров. Возможно, они и не вполне отражают те ситуации, которые возникают в вашей практической деятельности, тем не менее вы сможете применить рассматриваемые в них понятия в возникающих у вас ситуациях.

Ниже приведено краткое описание содержания этой книги.

Глава 1, “Анализ пакетов и основы организации сетей”. В этой главе поясняется, что такое анализ пакетов, как он действует и как проводится. Здесь также даются основы передачи данных по сети и анализа пакетов.

Глава 2, “Подключение к сети”. В этой главе рассматриваются различные методики подключения анализатора пакетов к сети.

Глава 3, “Введение в Wireshark”. В этой главе даются основные сведения о приложении Wireshark. В частности, где его взять, как им пользоваться, что оно позволяет делать, чем оно примечательно и прочие полезные сведения о нем. В настоящее издание включено обсуждение вопросов специальной настройки Wireshark с помощью профилей конфигурации.

Глава 4, “Обработка перехваченных пакетов”. Установив и настроив Wireshark, вы, вероятно, захотите узнать, как взаимодействовать с перехваченными пакетами. В этой главе даются основы обработки перехваченных

пакетов, включая новые разделы с более подробным описанием особенностей отслеживания потоков пакетов и преобразования имен.

Глава 5, "Дополнительные возможности Wireshark". Научившись ползать, пора учиться летать. В этой главе подробно рассматриваются дополнительные возможности Wireshark, а также демонстрируется внутренний механизм действия некоторых менее очевидных операций. В эту главу включены новые разделы с подробным описанием особенностей отслеживания потоков пакетов и преобразования имен.

Глава 6, "Анализ пакетов из командной строки". Wireshark — замечательное средство, но иногда требуется оставить удобства графического пользовательского интерфейса, чтобы взаимодействовать с пакетами в режиме командной строки. В этой новой главе показывается, как пользоваться TShark и `tcpdump` — двумя самыми лучшими инструментальными средствами командной строки для анализа пакетов.

Глава 7, "Протоколы сетевого уровня". В этой главе демонстрируется, как обычная передача данных, выполняемая на сетевом уровне, выглядит на уровне пакетов, исследуемых в сетевых протоколах ARP, IPv4, IPv6 и ICMP. Чтобы устранять неполадки в этих сетевых протоколах на практике, следует сначала понять, каким образом они действуют.

Глава 8, "Протоколы транспортного уровня". В этой главе рассматриваются два наиболее распространенных сетевых протокола транспортного уровня: TCP и UDP. Оба эти протокола служат для передачи большинства рассматриваемых здесь пакетов, и поэтому очень важно уяснить, как они выглядят на уровне пакетов и чем они отличаются.

Глава 9, "Распространенные протоколы верхнего уровня". В этой главе продолжается рассмотрение сетевых протоколов и демонстрируется, как выглядят четыре наиболее распространенных протокола верхнего уровня: HTTP, DNS, DHCP и SMTP.

Глава 10, "Основные реальные сценарии". В этой главе представлен анализ некоторых примеров типичного сетевого трафика в первом ряде реальных сценариев. Каждый сценарий представлен в удобном для исследования формате, позволяющем выявить затруднение, возникшее в сети, проанализировать его и найти решение. В этих основных сценариях задействовано совсем немного компьютеров и проводится ограниченный анализ, но и этого должно быть достаточно, чтобы ввести вас в курс дела.

Глава 11, "Меры борьбы с медленной сетью". Наиболее характерные осложнения, с которыми приходится иметь дело сетевым техникам, обычно связаны с низкой скоростью работы сети. Эта глава посвящена решению подобного рода осложнений.

Глава 12, "Анализ пакетов на безопасность". Безопасность сетей является самым насущным предметом в области информационных технологий. В этой главе представлены некоторые сценарии, связанные с решением вопросов, имеющих отношение к безопасности, по методикам анализа пакетов.

Глава 13, "Анализ пакетов в беспроводных сетях". В этой главе даются основы анализа пакетов в беспроводных сетях. В ней обсуждается отличия анализа пакетов в беспроводных сетях от проводных, включая некоторые примеры трафика в беспроводных сетях.

Приложение А, "Дополнительная информация". В этом приложении представлены дополнительные инструментальные средства и ресурсы Интернета, которые могут оказаться полезными для дальнейшего применения методик анализа пакетов, усвоенных в этой книге.

Приложение Б, "Интерпретация пакетов". Если требуется подробнее изучить особенности интерпретации отдельных пакетов, то в этом приложении дается краткий обзор хранения пакетной информации в двоичном виде и ее преобразования в шестнадцатеричное представление. В этом приложении показывается также, как разбирать вручную пакеты, представленные в шестнадцатеричном виде, с помощью схем пакетов. Это удобно в том случае, если приходится уделять немало времени анализу специальных протоколов или пользоваться инструментальными средствами анализа пакетов в режиме командной строки.

Как пользоваться этой книгой

- **Как учебным пособием.** В таком случае читайте ее последовательно главу за главой, уделяя особое внимание реальным примерам в последующих главах, чтобы постепенно усвоить порядок анализа пакетов.
- **Как справочным пособием.** Некоторыми средствами Wireshark вам придется пользоваться нечасто, и поэтому вы можете забыть, каким образом они действуют. Поэтому иметь эту книгу под рукой очень удобно, чтобы освежить в памяти порядок применения отдельных средств Wireshark. Когда вы проводите анализ пакетов на своей работе, у вас может возникнуть потребность обратиться за справкой к диаграммам, схемам и методикам, представленным в этой книге.

О примерах файлов перехвата

Все файлы перехвата, употребляемые в примерах из этой книги, доступны на веб-странице издательства No Starch Press, посвященной этой книге, по адресу `https://www.nostarch.com/packetanalysis3/`. Чтобы извлечь

наибольшую пользу из книги, загрузите эти файлы и пользуйтесь ими, прорабатывая приведенные в ней практические примеры.

Фонд поддержки технологий в сельской местности

Во введении к этой книге нельзя не упомянуть о самом главном, что дало ее издание. Вскоре после выхода в свет первого издания я основал общественную организацию под названием "Фонд поддержки технологий в сельской местности" (Rural Technology Fund — RTF).

Современные информационные технологии обычно доступны учащимся в сельской местности — даже с отличной успеваемостью — в меньшей степени, чем в крупных городах. Основание "Фонда поддержки технологий в сельской местности" в 2008 году стало верхом всех моих мечтаний. Тем самым я пытался восполнить цифровой пробел между жителями сельской и городской местности. С этой целью в "Фонде поддержки технологий в сельской местности" действуют специальные учебные программы, мероприятия по привлечению жителей сельской местности, сбору пожертвований на ресурсы по обучению цифровым технологиям, проводятся учебные курсы и пропагандируются современные технологии в сельских и бедных районах.

В 2016 году "Фонд поддержки технологий в сельской местности" передал ресурсы по обучению цифровым технологиям в руки более 10 тыс. учащихся в сельских и бедных районах США. И мне приятно объявить, что весь свой авторский гонорар я направил на эти цели в Фонд. Если вы желаете узнать больше об этой общественной организации или принять посильное участие в ее деятельности, посетите ее веб-сайт по адресу `http://www.ruraltechfund.org/` или найдите ее в Twitter по адресу `@RuralTechFund`.

Как связаться с автором книги

Мне всегда любопытно знать, что читатели думают о моей книге. Если вы желаете связаться со мной по какой-нибудь причине, направляйте все свои вопросы, комментарии, замечания и предложения прямо мне по адресу `chris@chrissander.org`. Кроме того, я регулярно веду свой блог по адресу `http://www.chrissanders.org/`, и меня можно найти в Twitter по адресу `@chrissanders88`.

От издательства

Вы, читатель этой книги, и есть главный ее критик и комментатор. Мы ценим ваше мнение и хотим знать, что было сделано нами правильно, что можно было сделать лучше и что еще вы хотели бы увидеть изданным нами. Нам

интересно услышать и любые другие замечания, которые вам хотелось бы высказать в наш адрес.

Мы ждем ваших комментариев и надеемся на них. Вы можете прислать нам бумажное или электронное письмо, либо просто посетить наш веб-сайт и оставить свои замечания там. Одним словом, любым удобным для вас способом дайте нам знать, нравится или нет вам эта книга, а также выскажите свое мнение о том, как сделать наши книги более интересными для вас.

Посылая письмо или сообщение, не забудьте указать название книги и ее авторов, а также ваш обратный адрес. Мы внимательно ознакомимся с вашим мнением и обязательно учтем его при отборе и подготовке к изданию последующих книг.

Наши электронные адреса:

E-mail: info@williamspublishing.com

WWW: http://www.williamspublishing.com