01 Общие сведения об аудите информационных систем

На данный момент существует множество материалов, посвященных различным методам взлома информационных систем (ИС) и проникновения в них, большая часть которых представляет собой набор готовых шагов и обещает быстрый результат. Что же на самом деле отличает вас как специалиста от тех, кто работает преимущественно с такими источниками? Ответ может показаться скучным и банальным, но все же скажем: это методологический подход, знание и понимание того, что происходит.

При написании этой книги была поставлена задача не просто рассмотреть определенный набор инструментов, но дать читателю глубокие знания, позволяющие адаптировать работу этих инструментов к каждой конкретной задаче и в целом сделать работу более продуктивной.

Книга не претендует на то, чтобы стать полным и исчерпывающим руководством в сфере информационной безопасности (ИБ), главной ее задачей является знакомство с основными концепциями и примерами. После ее прочтения вам предстоит провести достаточно много времени, совершенствуя свои знания и полученные навыки, но за интересной работой и время летит незаметно, не так ли?

Для тех, кто только делает свои первые шаги в области информационных технологий (ИТ), книга может оказаться сложной для понимания. Она предполагает, что у вас есть некоторый опыт работы с основными сетевыми сервисами и вы как минимум не боитесь командной строки Linux. Справедливости ради стоит добавить, что иногда знание стандартов мешает мыслить вне рамок. Но все же без знания принципов работы операционных систем (ОС), компьютерных сетей, базовых навыков программирования вам будет достаточно сложно войти в сферу ИБ.

Стоит отметить, что в последнее время специалистам в сфере ИБ пришлось освоить еще одну специализацию — управление проектами. В современном мире в связи с постоянным увеличением доступной информации специализа-

ция постоянно становится все более узкой, не миновало это и сферу ИБ. Если в Средние века один врач мог лечить практически все, то в наше время есть определенные специалисты: невролог, кардиолог, ревматолог, нейрохирург и т. д. То же самое касается и ИБ: вы обязательно встретите профессионалов, специализирующихся в основном на поиске информации, веб-приложениях или аппаратном взломе. Когда вы получите контракт на аудит большой и сложной ИС, вам придется руководить всеми этими специалистами, делать так, чтобы они работали слаженно и эффективно. Руководство проектами выходит за рамки темы этой книги, но мы настоятельно рекомендуем вам ознакомиться с основами этой работы.

Вопросы этики

В мире информационной безопасности присутствует условное разделение занимающихся взломом ИС людей на три группы: «черные шляпы» («Black Hat»), «серые шляпы» («Gray Hat») и «белые шляпы» («White Hat»). В чем же принципиальное различие между ними? На первый взгляд в соблюдении этических принципов. Ведь одни занимаются незаконной деятельностью, а другие соблюдают принятые нормы. Но на самом деле главное отличие «черных» от «белых» состоит в получении разрешения. «Черные» занимаются взломом и проникновением в ИС без какого-либо согласования, а «белые» делают это с разрешения владельца системы.

В данном контексте стоит упомянуть историю Адриана Ламо (Adrian Lamo). Он взламывал информационные системы организаций без их ведома и согласия, но каждый раз после удачного проникновения создавал подробный отчет о своей работе и отправлял его владельцам ИС с рекомендациями по устранению недостатков. И все же, несмотря на многочисленные благодарности, широкое признание в определенных кругах и этичное поведение, ему не удалось избежать уголовного преследования и реального тюремного срока. Этот случай демонстрирует, что даже «черные шляпы» могут действовать этично.

Для некоторых специалистов вопросы этики остаются скучными и непонятными, известными лишь из презентаций или вебинаров, однако для тех, кто относит себя к категории «белых шляп», они являются фундаментальными. «Белые шляпы» не только стараются соблюдать этические принципы, но и активно продвигают свои идеи в обществе.

Так, Консорциум интернет-систем (Internet Systems Consortium) — одна из организаций, занимающихся вопросами информационной безопасности, — определяет основные этические каноны следующим образом:

- защищайте общество, общественное благо, общественное доверие и инфраструктуру;
- действуйте честно, справедливо, ответственно и законно;

- выполняйте служебные обязанности добросовестно и профессионально;
- развивайте и защищайте профессию.

Необходимо всегда ставить вопросы этики во главу угла; вам часто придется делать выбор, основываясь исключительно на внутреннем чувстве справедливости, и к сожалению, не всегда правильный выбор будет самым простым и удобным.

Черные шляпы

В сфере ИБ «черными шляпами» называют тех, кто проникает в информационные системы без получения предварительного согласия. Некоторые делают это по финансовым соображениям, кто-то из спортивного интереса — причин на самом деле может быть много, и не стоит всегда сводить мотивацию лишь к одной из них.

Часто случается так, что действующие на территории одной страны в рамках ее правового поля специалисты по ИБ могут при этом нарушать законодательство другой страны. В этом случае их действия все равно будут считаться незаконными и могут повлечь серьезные последствия. Это хорошо иллюстрирует случай с Дмитрием Скляровым. Его работа была связана с обходом методов защиты электронных книг, разработанной компанией Adobe. Дмитрий был арестован по приезде в США на конференцию по информационной безопасности, так как его действия нарушили законы этой страны (несмотря на то, что по закону своего государства он не считался преступником).

Иногда можно стать преступником, даже выполняя вполне законные действия. В некоторых компаниях есть специальные программы, которые позволяют осуществлять поиск уязвимостей без предварительного согласования, но и тут не все так просто. Майкл Линн (Michael Lynn) нашел уязвимость в продукте корпорации Cisco и хотел представить ее на одной из конференций по ИБ. Когда представители компании узнали об этом, они подали на исследователя в суд с целью запретить ему выступать с таким докладом. Несмотря на достигнутое соглашения, он все же выступил с запланированной темой. После он получил судебный запрет на дальнейшее раскрытие информации о полученной уязвимости. Тут мы опять сталкиваемся с этическим вопросом — считать его злоумышленником или нет?

Также известны случаи, когда после успешно проведенных атак, нацеленных на проникновение в ИС, специалистам удавалось избежать судебного преследования и они устраивались на хорошо оплачиваемые должности.

Трудности с точной классификацией обусловлены тем, что в ее основу положен признак, по-разному оцениваемый с различных точек зрения. В этой книге остановимся на том, что «черные шляпы» — это те, кто совершает незаконные действия.

Белые шляпы

В подавляющем большинстве это специалисты, которые осуществляют аудит безопасности информационных систем по предварительному согласию обеих сторон, под коим обычно подразумевается трудовой договор или договор на оказание услуг. Все законно и не связано с какими-либо этическими или правовыми конфликтами.

Многих больше всего интересует вопрос, кто же обладает лучшими навыками взлома и проникновения — «белые шляпы» или «черные»?

На самом деле не все так просто. Обычно те, кто занимается законным аудитом, более профессиональны. Часто это сотрудники крупных фирм или компаний, специализирующихся на предоставлении услуг в области ИТ и ИБ, которые могут вкладывать средства в обучение своих работников. Следовательно, они получают доступ к лучшим материалам и с ними работают опытные инструкторы. Также у «белых шляп» есть возможность на практике познакомиться с различными продуктами обеспечивающих ИБ компаний, протестировать новое оборудование и протоколы.

Однако и на них накладываются определенные ограничения. Во-первых, как уже упоминалось, они связаны этическими и правовыми нормами. Второй момент связан с техническими аспектами. Часто выполнение тестов на проникновение может привести к потере данных, отказу в обслуживании и другим неприятностям, способным парализовать работу предприятия. В связи с этим «белые шляпы» несколько ограничены в методах и не всегда идут до конца.

Серые шляпы

Как уже было сказано, отнесение специалиста к той или иной категории иногда зависит от точки зрения. Это справедливо и в отношении «серых шляп». Такие специалисты по большей части действуют в рамках закона, но иногда могут незначительно выходить за его пределы. Так, некоторые специалисты могут осуществлять взлом коммерческого программного обеспечения (ПО), но делают это не для извлечения прибыли или публикации результатов своей работы. Вот таких специалистов и можно отнести к данной категории.

Взлом или аудит?

Раз уж мы начали говорить о терминологии, затронем еще один термин — «взлом». Взлом — это незаконное проникновение в систему, тогда как тест на проникновение — законное действие. Конечно, это деление условно, ведь все зависит не от терминологии, а от того, в каком контексте происходит данное действие.

А вот аудит информационных систем сильно отличается от взлома и даже от теста на проникновение. Во-первых, понятие аудита применимо только к за-

конным действиям. Во-вторых, если тест на проникновение означает поиск уязвимости и ее последующую эксплуатацию, то аудит предусматривает поиск и возможную эксплуатацию всех найденных аудитором уязвимостей. Тесты на проникновение означают, что хакер изначально ничего не знает о внутренней сети предприятия — так называемый метод черного ящика («Black Box»). В аудите предусмотрены методы как «черного ящика», так и «белого ящика» («White Box»), когда аудитор получает доступ к конфигурации и полной информации обо всех ИС предприятия. В данной книге рассмотрены только методы «Black Box».

Автор надеется, что читатели будут использовать информацию из данной книги только в целях законного взлома ИС. Пожалуйста, помните о неотвратимости наказания — любые незаконные действия влекут за собой уголовную или административную ответственность.

Разрешение на взлом

Вы уже наверняка заинтересовались вопросом, а может ли взлом быть законным? Конечно может! Законным взлом информационных систем является в нескольких случаях:

- вы взламываете принадлежащие вам ИС;
- аудит информационной безопасности сети предприятия входит в ваши должностные обязанности;
- вы взламываете сеть организации, с которой у вас заключено письменное соглашение о проведении аудита или тестов на проникновение.

Поскольку в первых двух случаях все достаточно просто, мы не будем заострять свое внимание на их рассмотрении, а разберемся со случаем, когда вас нанимают для проведения внешнего аудита ИС. В этой ситуации перед началом работ вы должны будете заключить несколько соглашений, которые и рассмотрим подробнее.

Соглашение о неразглашении

Скорее всего, вы уже встречались с таким типом документов. Основная его суть заключается в том, что вы обязуетесь не разглашать любую информацию, полученную в ходе проведения аудита ИС заказчика. Обычно это относится не только к промежутку времени, в который проводятся работы, действие таких соглашений может растягиваться на десятилетия. Соглашения могут также содержать специальный пункт о хранении, обработке и методах уничтожения данных. Будьте готовы к тому, что вас могут попросить уничтожить специально оговоренным методом жесткие диски, на которых хранилась информация, и предоставить тому документальное подтверждение. Справедливости ради следует сказать, что это скорее исключение, нежели правило.

Под действие этого соглашения подпадают абсолютно все информационные потоки, которые создавались в ходе вашей работы. Это распространяется на снимки экранов, подготовленную документацию, включая все черновики, историю командной строки, коммуникации по электронной почте, любые документы (финансовые отчеты, маркетинговые планы, конфигурационные файлы и т. д.), полученные вами в ходе тестирования или переданные вам заказчиком, а также многое другое.

Попробуйте поставить себя на место заказчика. Вы нанимаете команду специалистов, которая проникает в вашу сеть разными способами, получает права администратора в вашей системе и доступ к внутренней информации. На разглашение какой доли данных вы могли бы дать согласие?

Обязательства заказчика

В данном разделе прописано, что, каким образом и как должен делать заказчик во время действия этого договора. Ни для кого не секрет, что заказчик всячески будет стараться оберегать себя и получить от вас максимум за свои деньги, — это нормально. Помните, что вы всегда должны внимательно читать все, что собираетесь подписать, и у вас есть полное право не соглашаться на выполнение работ, которые не принесут вам какой-либо выгоды. Из вашего сотрудничества каждая сторона должна извлечь для себя пользу.

Не стоит удивляться тому, что в таких договорах вы встретите информацию о том, каким образом будет происходить ваша работа и как заказчик будет за вами наблюдать. Самый простой способ — сбор записей с вашей стороны и со стороны заказчика обо всех ваших действиях. Таким образом заказчик будет стараться оградить себя от возможных рисков утечки информации, а в случае, если во время тестов произойдет сбой в системе, он будет знать, кто за это ответствен.

Другим способом защиты является наблюдение. Когда вы будете проводить аудит в помещении заказчика, к вам могут приставить специально обученного человека. Не стоит волноваться, у таких людей нет цели скомпрометировать вас или узнать секреты вашей работы. Обычно они следят за тем, чтобы вы ненароком не получили доступ к той информации, которая может считаться секретной. И это касается не только ИС — например, вы случайно можете свернуть не туда и попасть в конференц-зал, где обсуждаются будущие бизнес-стратегии. Плюс в наличии такого сопровождающего заключается в том, что если вы найдете критическую уязвимость, которую, на ваш взгляд, стоит исправить безотлагательно, вы можете сразу сообщить ему об этом — необходимые действия по устранению начнутся гораздо быстрее.

Иногда бывает и так, что заказчик обязуется предоставить вам все необходимое оборудование и программное обеспечение за свой счет. И это не потому, что вы ему понравились и он хочет купить вам новый компьютер в счет еще не выполненной работы — все купленное, к сожалению, остается в его собственности. Это делается в тех случаях, когда вы проводите аудит в помещениях заказчика

и можете выполнять работу только на принадлежащем заказчику оборудовании, которое не должно покидать стены организации.

В авторитетных источниках упоминается (хотя сам автор с этим не сталкивался), что в некоторых случаях заказчик не только настаивает на проведении аудита на принадлежащем ему оборудовании, но также запрещает проносить с собой любые устройства, которые могу обеспечить хранение, обработку или передачу данных.

Обязательства исполнителя

Помимо требований соблюдения вами конфиденциальности в отношении данных заказчика, в соглашении также может содержаться информация о том, каким образом вы можете распоряжаться полученными данными и кому вы можете их передавать. Обычно это подразумевает, что вы должны передать результаты вашей работы определенному кругу лиц (это могут быть назначенные сотрудники и руководство предприятия). Кроме того, в некоторых случаях добавляется пункт, в котором оговаривается, каким третьим сторонам и какую информацию вы можете передавать.

Отнеситесь к этому внимательно и всегда проверяйте информацию о том, кому вы передаете данные. Часто бывает так, что аудит занимает несколько месяцев, а за это время человек, которому вы должны передать данные, может сменить место работы. Поэтому, чтобы не нарушить соглашение о неразглашении, убедитесь, что он до сих пор является сотрудником организации и у него все еще есть право доступа к той информации, которую вы хотите ему передать.

Часто в этом пункте также будут оговариваться действия, которые вы можете или не можете производить во время выполнения заказа. Например, вам могут запретить создание новых пользователей в системе, оговорить, какими способами вы может аутентифицироваться, к каким данным вы может получить доступ и многое другое. Скорее всего, вам будет запрещено использовать любые вирусы и другие вредоносные программы, а также проводить атаки, способные вызвать отказ в обслуживании.

Если же вы не видите вышеописанного в договоре, то не спешите радоваться — вполне возможно, что, подписав такой договор, вы подвергнете себя риску. Часто описание всего вышесказанного замещается дежурным «все необходимые действия», а это в каждом случае можно трактовать по-разному. Например, было ли использование эксплойта необходимым действием? Вы считаете, что да, а вот заказчик может иметь совершенно другое мнение на этот счет. Не пожалейте своего времени и заранее оговорите все как можно более детально.

Аудит и мониторинг

В контексте договора об исполнении услуг имеется в виду не аудит инфраструктуры вашего заказчика, а именно аудит ваших систем, цель которого — убедить-

ся, что условия договора не нарушены. Обычно заказчик хочет удостовериться в том, что данные, которые вы получаете, хранятся и обрабатываются в безопасном месте, а каналы передачи надежно защищены. Клиент хочет быть уверен, что ваша лаборатория представляет собой образцовое рабочее место в плане ИБ, вы же в этом разбираетесь, не так ли?

Под мониторингом также подразумевается, что будут следить именно за вами и вашими действиями. Заказчик хочет быть уверен, что вы соблюдаете условия договора и не производите никаких действий, не предусмотренных подписанным соглашением. Однако учтите, что не всегда вы сможете действовать в рамках установленных соглашений. Возможны и случаи, когда вам будет необходимо провести не предусмотренные соглашением или не оговоренные заранее мероприятия. Всегда согласовывайте их перед проведением. Помните, что устные договоренности могут ничего не значить, вы всегда должны получить подписанное разрешение. Чтобы это не превратилось в головную боль и не занимало много времени, заранее обговорите с заказчиком процедуру получения таких разрешений.

Разрешение конфликтов

Разногласия — обычное дело при проведении любых работ, и многие из них можно решить в процессе переговоров. Возможно, вам не удалось выполнить часть задач из-за технических ограничений. Также бывали случаи, когда недовольные ИТ-специалисты пытались прикрыть недостатки своей работы действием ИБ-аудиторов, — будьте готовы и к этому.

Однако в случае, когда стороны не могут договориться, процедура разрешения споров переходит на новый, уже юридический уровень. Поэтому внимательно отнеситесь к этому пункту.

Порядок проведения аудита

Любой профессионал по информационной безопасности хочет заниматься своим любимым делом на законных основаниях. Чаще всего такие люди являются частью команды, проводящей комплексный аудит безопасности информационных систем предприятий; реже они устраивают тесты на проникновение в индивидуальном порядке.

Чтобы быть уверенным в правильности и законности своих действий, профессионал должен соблюдать следующие правила:

- получать от клиента письменное разрешение на проведение тестов на проникновение или аудита ИС;
- соблюдать соглашение о неразглашении информации;
- гарантировать, что никакая информация, полученная во время работы с клиентом, никогда не станет известной другим лицам;
- проводить все тесты, согласованные с клиентом, и никакие другие.

Аудит информационных систем обычно проходит в несколько этапов:

- встреча с клиентом, обсуждение целей и средств;
- подписание договора о неразглашении информации;
- подписание договора об оказании услуг;
- сбор группы участников аудита, распределение ролей и подготовка расписания тестов;
- проведение тестов;
- анализ и проверка полученных результатов;
- подготовка отчета;
- передача отчета клиенту.