АВТОР: АНДРЕЙ ВЛАДИМИРОВ, CSO ARHONT LTD (WWW.ARHONT.COM)

Внутренний VS внешний аудит безопасности

ТЕХНИЧЕСКИ, ВНУТРЕННИЙ АУДИТ ИТ-БЕЗОПАСНОСТИ КОМПАНИИ ИЛИ ОРГАНИЗАЦИИ ОТЛИЧАЕТСЯ ТЕМ, ЧТО АУДИТОРЫ ИЗНАЧАЛЬНО ИМЕЮТ ДОСТУП К СЕТЕВЫМ РЕСУРСАМ ИЗНУТРИ, Т. Е. С «ЧИСТОЙ СТОРОНЫ» МЕЖСЕТЕВОГО ЭКРАНА.

АВТОР: АНДРЕЙ ВЛАДИМИРОВ, CSO ARHONT LTD (WWW.ARHONT.COM)

Чаще всего это означает авторизованное подключение лэптопов и других мобильных хостов аудиторов к портам корпоративных коммутаторов. Как вариант, возможна выдача непривилегированных аккаунтов на пользовательских системах или серверах компании с целью выяснения вероятности получения административного доступа к этим системам и дальнейшего проникновения в тестируемые сети и их узлы благодаря открывшимся возможностям. Изредка удаленные аудиторы получают авторизованный доступ к внутренним ИТ-ресурсам посредством ВЧК или же через беспроводную сеть. Допустимы сочетания внутреннего и внешнего (дальнейшее тестирование безопасности локальной сети, используя прорехи, найденные в процессе удаленной проверки защищенности ее периметра), внутреннего и беспроводного (фактически, атака проводной сети с беспроводной, к которой был ранее получен доступ), внутреннего и физического (непосредственный доступ ко внутренним сетевым ресурсам не авторизован и осуществляется посредством социальной инженерии) аудитов. При подготовке к проверке компании на соответствие требуемым стандартам, таким как ISO 27001:2005 или PCI DSS, внутренний аудит безопасности в первую очередь служит для выявления и корректировки несоответствий реальных сетей и систем положениям корпоративной политики безопасности, основанным на ней целеуказаниям, руководствам и схемам по защите информации. Во всех перечисленных комбинациях внутренний аудит безопасности можно рассматривать как вторую фазу общей проверки информационной безопасности организации или компании.

Кому нужен аудит

Если подходить к этому вопросу формально, то в первую очередь проверка безопасности изнутри нужна компаниям, многим сотрудникам которых по определению нельзя доверять. Это могут быть, например, компании с высокой ротацией персонала, полагающихся на временных работников, а также контрактников, набираемых под отдельно взятые проекты. Однако, если задуматься, какая крупная организация может доверять всем своим сотрудникам до единого и строго контролировать их действия внутри локальной сети? Ничто не вечно под Луной, и даже наиболее проверенный и уважаемый работник сегодня или завтра может встать на тропу войны против своих работодателей и коллег под влиянием самых разных факторов, от личных конфликтов и обид до компромата и шантажа со стороны третьих лиц. А если посмотреть на проблему еще шире, то как только внешний атакующий получил возможность выполнять команды на любом из внутренних хостов или посылать пакеты внутри локальной сети, он по определению становится внутренним. В теории проведенный по всем правилам удаленный аудит безопасности с последующим устранением найденных проблем должен пресекать такие инциденты на корню.

Но на практике далеко не все так гладко. В придачу никто не отменял zero-day эксплойты, множащиеся с каждым днем атаки на клиентские приложения (в особенности веб-браузеры), социальную инженерию, беспроводной взлом (все ли клиентские 802.11 устройства вашей компании учтены и защищены), старый добрый wardialing (соединения dial-in к маршрутизаторам до сих пор часто используются для их внеканальной резервной администрации) и лобовое физическое проникновение с подключением к локальной сети. Удаленный аудит безопасности периметра сети значительно снижает вероятность успеха атак «в лоб», но «умный в гору не пойдет, умный гору обойдет». Таким образом, искренний ответ на поставленный в заголовке вопрос — всем, кто обладает развитой сетевой инфраструктурой и относится к информационной безопасности серьезно. Надежная оборона обязана быть эшелонированной.

Сложившаяся на настоящий момент ситуация парадоксальна. Согласно статистике FBI, CERT и множества других служб и организаций, порядка 70% успешных взломов происходит изнутри. Да и большинство расследований компьютерных преступлений, в которых довелось принимать участие автору данной статьи, относилось как раз ко внутренним атакам на почве конфликтов при увольнении сотрудников, борьбы за должности при слиянии корпораций и тому подобного. Такие атакующие уже обладают как минимум правами обычного пользователя (в одном из упомянутых выше расследований нам удалось выяснить и доказать, что взломщик — бывший ИТ-директор одной из двух сливающихся компаний), они более мотивированы, упорны и знают, что именно им нужно достичь. В то же время львиная доля заказываемых аудитов ИТ-безопасности — удаленные, внешние и абсолютно бесполезные в описываемых ситуациях. «Защищайся там, где не нападают», — писал Сун Цзы и, словно следуя этому девизу, владельцы корпоративных сетей концентрируют меры противодействия на их периметре, который в гораздо меньшей мере подвержен успешным, высокоэффективным атакам, чем «мягкое подбрюшье» таких сетей (постоянные попытки просканировать порты, новички и черви, ищущие старые незалатанные системы не в счет). Однако крылатая фраза древнекитайского стратега имеет и вторую половину: «Нападай там, где не защищаются». И пока перевес явно на стороне нападающих.

Ключевые различия

Мало того что частота проводимых внутренних аудитов информационной безопасности значительно уступает числу внешних, даже если речь идет о многонациональных корпорациях, так в подавляющем количестве случаев эти аудиты осуществляются с использованием подходов, методологии и отчетных форматов, полностью идентичных таковым при удаленном тестировании. При этом в достаточной мере не учитываются ни специфика, связанная с нахождением аудитора внутри локальной сети клиентской компании или организации, ни значительные преимущества, которые подобная позиция предоставляет атакующему. Ведь отсутствие межсетевого экрана на пути к заветным целям, наличие программных уязвимостей, которые можно использовать только локально, и частое присутствие внутри сетевого периметра «полузабытых» хостов со старыми уязвимыми версиями установленных операционных систем, сервисов и приложений — это далеко не все. Постараемся же разобраться, в чем заключаются остальные, не менее важные отличия между внутренней и внешней проверкой безопасности ИТ-инфраструктуры.

Во-первых, при проведении внутреннего тестирования безопасности сети аудитор имеет (или может легко получить) полный доступ к используемым в этой сети протоколам. Пассивная энумерация и фингерпринтинг операционных систем и сервисов хостов, уменьшающие интенсивность «шумного» активного сканирования? Нет проблем! Особенно когда в сети присутствуют такие протоколы, как CDP и SNMP. Нужно построить схему топологии сети? Нет нужды «пинговать» все возможные IP-адреса ARP- и ICMP-пакетами — тихо слушаем и анализируем протоколы маршрути-

АВТОР: АНДРЕЙ ВЛАДИМИРОВ, CSO ARHONT LTD (WWW.ARHONT.COM)

зации и резервные протоколы маршрутизации (VRRP и HSRP сразу покажут локальные шлюзы). Удаленный доступ без особого труда? Смотрим на незащищенные протоколы управления, такие как telnet и вышеупомянутый SNMP (до третьей версии при условии включения функций аутентификации и шифрования), ищем TFTP-пакеты с названиями конфигурационных файлов, использующих этот протокол сетевых устройств. Примитивно, но атакующие, особенно изнутри компании, не будут церемониться и искать сложные пути. Чуть более труден стандартный взлом плохо защищенных протоколов, к примеру SSHv1 (примите на заметку, что модификация SSHv1, используемая устройствами Cisco, с помощью sshmitm из Dsniff не ломается) и SSL/TLS-защищенных соединений, использующих CBC-режим (проект Omen). Можно еще вспомнить протоколы аутентификации, до сих пор применяющие MS-CHAPv1, а также старые добрые LM- и NTLM-хэши. К сожалению, вероятность столкнуться с подобными динозаврами на внутренних сетях по-прежнему велика, чтобы не сбрасывать их со счетов.

Отдельно стоит выделить тестирование на уязвимость к атакам, связанным с перенаправлением сетевого трафика и его дальнейшей модификацией (например, с помощью pdump и netsed, вставка записанных wavов в VOIP-потоки посредством vomit и т.п.). Тема атак «человек в середине» посредством подделки ARP-сообщений уже настолько заезжена, что, казалось, можно было бы ее и не упоминать. Но установлен ли на ваших сетях Arpwatch или иные средства защиты (например, использование «липкого ARP» или динамической ARP-инспекции на коммутаторах) от этой извечной проблемы? И даже если ответ на этот вопрос позитивен, не обольщайтесь. Есть множество других способов перенаправить трафик на локальной сети, не имеющих никакого отношения к ARP. Атакующий может легко установить фальшивый DHCP-сервер и подделывать DHCP сообщения. Он может попытаться отравить кэш вашего DNS-сервера (более распространенные атаки подделки идентификационных номеров DNS требуют успешной предварительной атаки «человек в середине» на более низких сетевых уровнях).

Но гораздо реже при проведении внутренних аудитов сетевой безопасности проверяют защищенность протоколов второго и третьего сетевого уровней, включая разнообразные протоколы маршрутизации (RIP, IGRP, EIGRP, OSPF, IS-IS, iBGPv4), уже упомянутые VRRP и HSRP, и протокол связующего древа (STP). Посредством злонамеренной инъекции пакетов/фреймов перечисленных протоколов атакующий может перенаправить трафик целого сегмента или даже автономной системы в нужном для него направлении (обычно через принадлежащий ему хост). Данная тема слишком широка для более подробного раскрытия в этой обзорной статье, поэтому просто отметим, что при проведении внутренних аудитов, по опыту, крайне редко встречаются сети, в которых все вышеперечисленные протоколы были бы как следует защищены. К примеру, даже если MD5-аутентификация протоколов маршрутизации была включена, пароли ломались по словарю либо была возможность использовать недостатки самого механизма аутентификации (атаки проигрывания RIP и EIGRP пакетов).

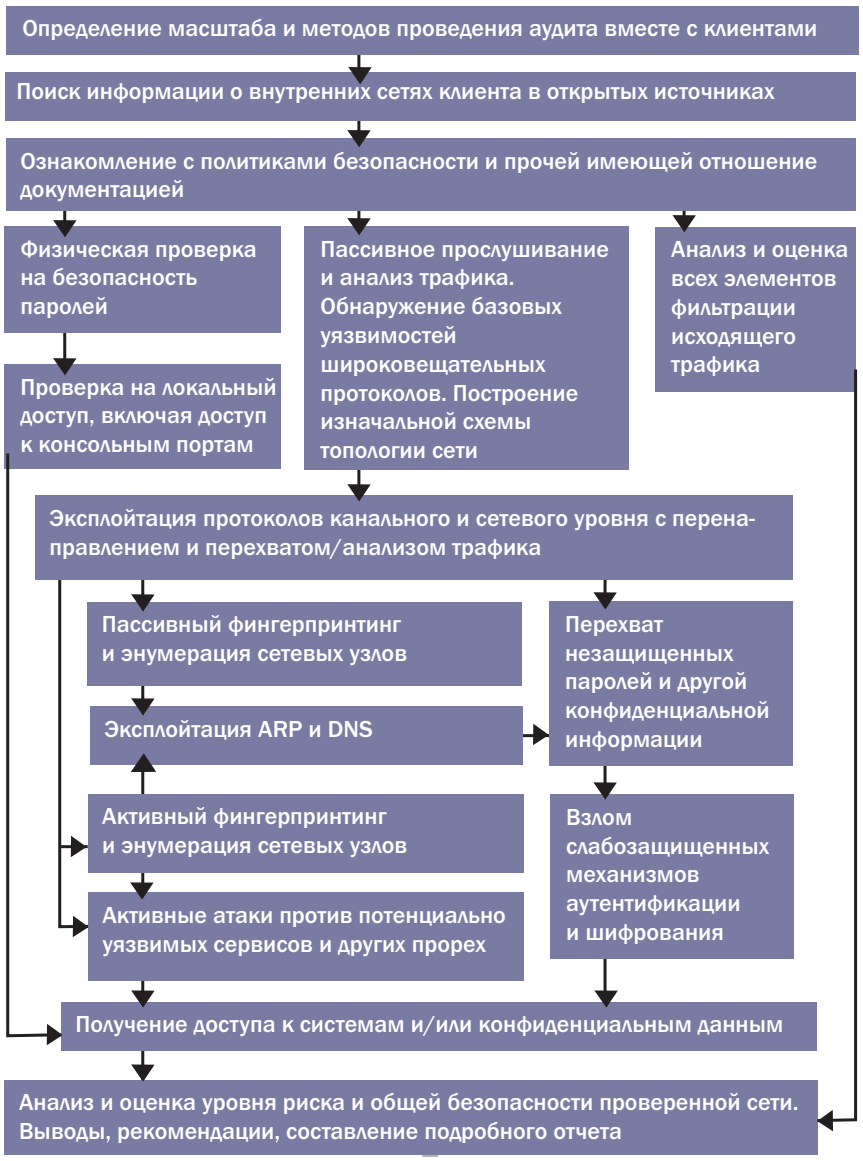
В заключение, говоря о тестировании безопасности низкоуровневых протоколов, невозможно не упомянуть «прыжки через виртуальные локальные сети (VLANs)». Многие до сих пор считают разделение на виртуальные локальные сети одним из элементов безопасности сетевой инфраструктуры. Не мудрствуя лукаво, скажем, что если атакующий может получить доступ к магистральному порту коммутатора, например, заставив порт, к которому подсоединен его хост, стать магистральным (через инъекцию DTP-пакетов на «сисках» и т. д.), то для него разделение на VLAN'ы более не проблема. Кроме того, для удобства администрации сетей с большим количеством VLANов многие пользуются «автоматическими» протоколами управления виртуальными локальными сетями, в частности VTP. В случае недостаточной защищенности VTP, локальный атакующий может получить полный контроль над VLAN'ами злосчастной сети, что не только устраняет их как барьер, но и открывает массу интересных возможностей. К примеру, можно отрезать от сети централизированный сервер журналирования или рабочую станцию системного администратора, посадив их на отдельный VLAN для времяпрепровождения в гордом одиночестве.

Помимо необходимости глубокой проверки защищенности сетевых протоколов есть и другие специфические элементы проведения внутренних аудитов ИТ-безопасности. Скажем, вы как аудитор предположили, что, находясь в локальной сети, вам более не стоит думать о брандмауэрах и прочих шлюзовых устройствах на ее периметре. Стоп. А как насчет тестирования фильтрации выходящего трафика? Если эгресс-фильтрование отсутствует напрочь, то компания крайне безалаберно относится к информационной безопасности, и в отчете после аудита можно смело подчеркивать это как серьезную проблему. Если же выходящий трафик фильтруется, нужно как следует проверить тщательность этой фильтрации, включая отсеивание вредоносных программ, генерируемого червями и DDoS утилитами трафика, спама и другого нежелательного контента (возможное содержание которого мы оставляем на волю вашего воображения). Выход подобных данных наружу может нанести серьезный ущерб имиджу предприятия и привести к неприятным юридическим последствиям.

Перед тестированием правил и методов эгресс-фильтрования проверьте политику/устав безопасности компании на предмет данных, запрещенных к выходу наружу, так как вариации подобных ограничений от компании к компании могут сильно отличаться. По большому счету полноценный внутренний аудит информационной безопасности должен быть сопряжен с проверкой политик и руководств безопасности и процессов управления ее обеспечением, равно как и по крайней мере самим базовым физическим аудитом. В конце концов искомый пароль может быть написан на клочке бумаги под клавиатурой тестируемой системы, в придачу незащищенной скринсэйвером и BIOS-паролем. Или же имеется возможность незаметно проскользнуть в серверную с консольным кабелем наперевес… И если все эти вещи, равно как и необходимость и параметры фильтрования выходящего трафика или положения по мерам защиты низкоуровневых протоколов, не прописаны в политике безопасности и другой, опирающейся на ней документации, есть хорошие шансы, что их просто проигнорируют. Посему отчет по внутреннему аудиту безопасности должен охватывать и административный аспект: внести, добавить, дополнить эти положения в вышеперечисленные документы на основании результатов проведенного тестирования.

В целом формат отчета по внутреннему аудиту никак не может быть идентичным отчету по аудиту удаленному. Полноценный отчет о проведенном аудите безопасности должен обязательно включать в себя такие элементы, как оценка риска и уровень умений атакующего для каждой найденной уязвимости. Это позволяет расставить приоритеты в закрытии обнаруженных прорех: дыры, не несущие особого риска и требующие при этом высокого уровня знаний для их эксплуатации, должны быть устранены в послед-

ОБЩАЯ СХЕМА ПРОВЕДЕНИЯ ВНУТРЕННЕГО АУДИТА ИТ-БЕЗОПАСНОСТИ



нюю очередь, а при недостатке времени и ресурсов могут быть и проигнорированы. Понятно, что и сами категории риска и «продвинутости» атакующего, и описывающие их шкалы (обычно приводятся в начальных общих разделах отчета) разительно отличаются для внутренних и внешних аудитов. Хотя бы из-за тех же атак на протоколы: в плане оценки риска невозможно сопоставлять SQL-инъекцию или кросс-сайт-скриптинг на удаленном сервере с перенаправлением и модификацией трафика в локальной сети или преодолением VLANов. Да и исходный набор знаний атакующего здесь полностью различен — программирование/администрация веб-приложений и баз данных с одной стороны и сетевая инженерия — с другой. Об оценке риска физических и процессуальных уязвимостей, часто обнаруживаемых при внутренних аудитах, можно и не говорить.

По большому счету и сами термины «удаленный»/«локальный» в описании обнаруженных прорех приобретают иное значение. Для внутреннего аудита удаленная уязвимость — это проблема безопасности другого хоста в локальной сети, для использования которой атакующему вполне может быть необходимо находиться в том же ее сегменте. Локальная уязвимость четко соотносится с дырой на самой тестируемой системе. А для категоризации уязвимостей протоколов или же некорректной фильтрации исходящего трафика придется вводить новый термин, скажем «сетевая уязвимость», с дальнейшей ее субкатегоризацией. Начальный раздел отчета, посвященный фингерпринтингу и энумерации сети перед тестированием и собственно во время тестирования на прорехи, также будет иным, включая описание пассивных методов, полную карту топологии сети, описание типов и потоков данных в ней. Включая вышеперечисленные, можно найти десятки отличий, обуславливающих разницу в форматах отчета по внешним и внутренним аудитам.

Подведем итоги

Внешний, удаленный аудит ИТ-безопасности и аудит внутренний — это, как говорят в Одессе, две большие разницы. Алгоритмы их проведения различны. Так, внутренний аудит должен начинаться с перехвата трафика и его анализа, пассивной энумерации и определения топологии сети. И только затем следует традиционное сканирование портов отдельно взятых систем, приоритеты тестирования которых выбраны на основе первой, пассивной фазы аудита. Наборы навыков аудиторов также отличаются — в связи с доступом к локальным сетевым протоколам знание и умение оценивать и проверять их безопасность становятся критическими и добавляются к типичному набору квалификаций, необходимых для удаленного тестирования. Безусловно, все вышеперечисленное вкупе с добавляющимися административными и физическими элементами аудита отражается на форме его отчетности, методологии и подходах к оценке характера уязвимостей, риска и уровня умений потенциальных атакующих.

Несмотря на понимание многими опасности атак изнутри и необходимости построения эшелонированной, многоярусной обороны, корректное и регулярное проведение внутренних аудитов безопасности по-прежнему является скорее исключением, чем правилом. И если данная статья заставит хотя бы задуматься над необходимостью уделять должное внимание внутренней оценке ИТ-безопасности и тому, как ее следует проводить, то ее задачу можно считать выполненной. it

АВТОР: АНДРЕЙ ВЛАДИМИРОВ, CSO ARHONT LTD (WWW.ARHONT.COM)