Итоги внешних тестирований на проникновение

Е.Д. Килюшева (Компания Positive Technologies)

Отмечена тенденция к увеличению доли комплексных проектов по проведению тестирования инфраструктуры компаний на проникновение с помощью пентестов. Приведены результаты анализа защищенности корпоративных информационных систем от внешних нарушителей. Сформулированы рекомендации, позволяющие повысить уровень информационной безопасности организации.

Ключевые слова: тестирование на проникновение, пентест, корпоративные информационные системы, уязвимости, учетные данные пользователей, Web-приложения.

Тестирование на проникновение — это моделирование действий реальных злоумышленников так называемыми этичными хакерами. Часто термин сокращают и называют такие работы пентестом, а экспертов, которые их проводят, пентестерами. В рамках пентеста специалисты по информационной безопасности (ИБ) ищут уязвимости в системах определенной компании и пытаются провести атаки в обход установленных средств защиты.

Когда тестирование проводится из внешних сетей (например, из сети Internet), пентест называют внешним. Если же моделируются атаки со стороны нарушителя, который находится внутри компании (например, с типовым набором привилегий сотрудника или от лица случайного посетителя), то пентест принято называть внутренним.

В последнее время наблюдается тенденция к увеличению доли комплексных проектов, когда компании проводят и внешний, и внутренний пентесты. При этом внутренний пентест может являться продолжением внешнего: такой подход позволяет оценить не только вероятность проникновения злоумышленника в локальную сеть, но и последствия развития атаки в инфраструктуре компании.

Пентестер должен иметь тот же уровень подготовки и те же инструменты, что и потенциальный злоумышленник. Из этого следует логичный вывод: чем выше уровень квалификации пентестера, тем лучше он может смоделировать действия профессионального хакера и тем качественней провести работу.

Важно отметить: в отличие от злоумышленников пентестер действует строго в рамках законодательства и только по согласованию с владельцем системы. Список атакуемых узлов и проводимые проверки обязательно согласовываются с ответственным представителем тестируемой компании.

Цель проведения тестирования на проникновение — оценка эффективности используемых систем защиты и готовности информационной инфраструктуры компании в целом к кибератакам. В рамках пентеста также можно оценить эффективность работы служб ИБ компании в выявлении и пресечении атак, если руководство не ставит их в известность о проводимых работах.

Ошибочно считать, что пентест направлен на выявление уязвимостей, ведь это не является его основной задачей. Пентестеры ищут недостатки безопасности, но только чтобы использовать их для достижения целей пентеста. Например, в случае внешнего тестирования задача обычно состоит в том, чтобы обнаружить максимальное число способов проникнуть в локальную сеть организации; в случае внутреннего — определить максимально возможный уровень привилегий, который может получить злоумышленник. Заказчик пентеста может дополнительно ставить и другие задачи (например, продемонстрировать возможность получения доступа к конкретным бизнес-системам).

Компании, заказывающие услуги пентеста. Пентест может быть полезен для любой организации независимо от сферы деятельности. Однако работы стоит проводить, когда в компании уже обеспечивается комплексная безопасность инфраструктуры, защищенность ее от кибератак, и внедрены средства защиты. Это означает, что уровень зрелости процессов ИБ в организации должен быть достаточно высоким. Особенно важно проводить тестирование на проникновение крупным компаниям с распределенной инфраструктурой, поскольку трудно обеспечить безопасность достаточно сложной системы без проверки эффективности ее защиты.

В 2019 г. среди всех организаций, для которых проводились пентесты, доля промышленных и энергетических компаний составила 25%.

Что дает пентест бизнесу

Современные подходы к организации бизнеса подразумевают оценку и управление бизнес-рисками. Руководители компаний четко понимают, какие из рисков наиболее значимы для их бизнеса сегодня. Многие из этих рисков могут быть реализованы в результате кибератаки (например, кража денег со счетов компании или срыв важного контракта в результате удаления файлов на компьютере директора).

Топ-менеджмент компании может обозначить эти ключевые риски команде пентестеров при проведении работ, и те проверят на практике, как и при каких условиях риски могут быть реализованы. Эксперты дадут рекомендации, как настроить инфраструктуру и какие системы защиты использовать, чтобы устранить или минимизировать именно эти риски.

Есть и другие аспекты, которые могут быть интересны бизнесу:

• *соответствие требованиям и рекомендациям регуляторов*, которые уделяют значительное внимание

ИБ, в том числе в свете закона о критической информационной инфраструктуре (КИИ);

• *эффективный выбор средств защиты и точек их применения в инфраструктуре* на основе информации о вероятном пути проникновения потенциального нарушителя и используемых им техниках атаки;

• *снижение затрат на защиту:* результаты пентеста позволяют ранжировать недостатки безопасности и направить ресурсы в первую очередь на устранение наиболее опасных угроз (то есть снизить риск компрометации систем и возможные затраты на устранение последствий атак в будущем);

• *репутация компании* как гаранта безопасности данных клиентов и партнеров может быть дополнительным преимуществом в бизнесе.

Результаты анализа защищенности корпоративных информационных систем от внешних нарушителей

Проанализируем результаты проектов по анализу защищенности корпоративных информационных систем от внешних нарушителей, выполненных в 2019 г. специалистами Positive Technologies (рисунок). Остановимся на наиболее распространенных недостатках безопасности и методах атак[1], а также дадим рекомендации по повышению уровня защищенности.

Для исследования были выбраны 28 проектов по внешнему тестированию на проникновение (из числа проведенных в тех компаниях, которые разрешили использовать обезличенные данные).

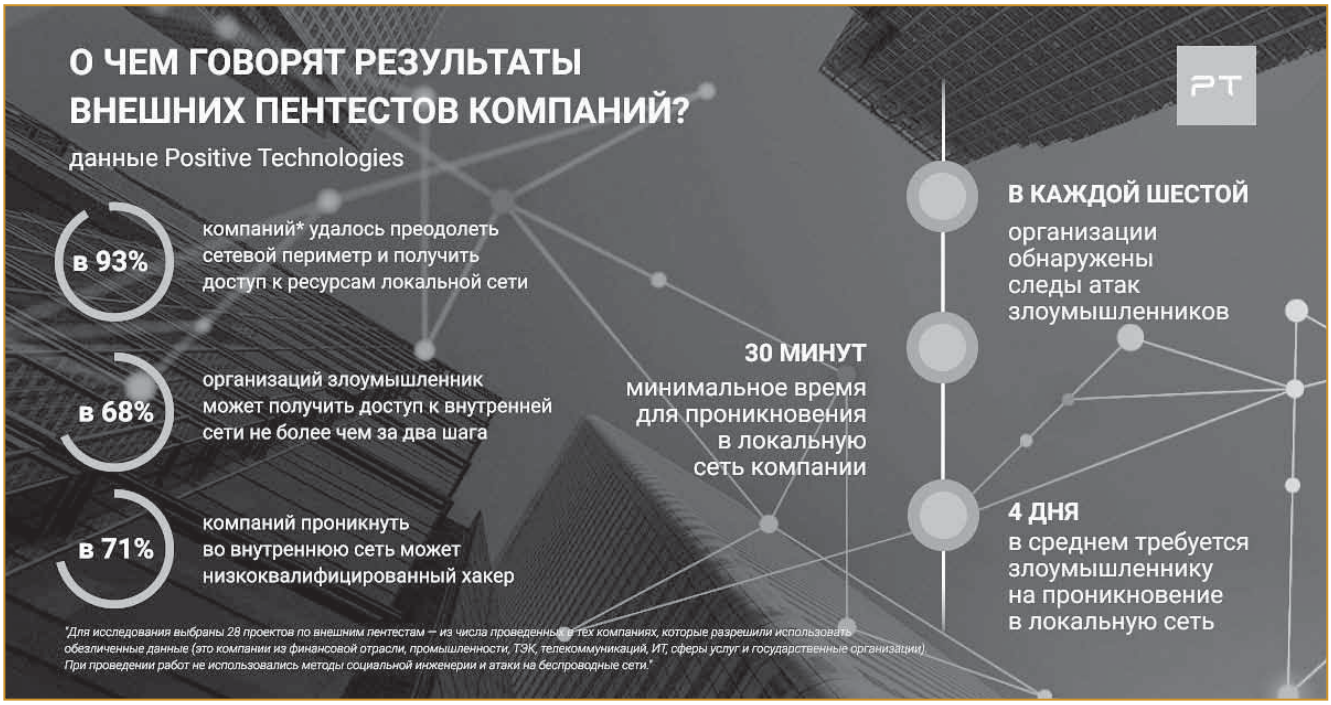
В ходе внешних пентестов преодолеть сетевой периметр и получить доступ к ресурсам локальной сети удалось в 93% организаций. Чаще всего существовало несколько способов преодолеть сетевой периметр: так, в среднем в одной компании выявлялось два вектора проникновения[2]. Максимальное число векторов проникновения, выявленных в одном проекте, — тринадцать.

На проникновение в локальную сеть требовалось в среднем четыре дня, а минимум — 30 мин. В большинстве случае сложность атаки оценивалась как низкая, то есть ее мог бы осуществить и низкоквалифицированный хакер, который обладает лишь базовыми навыками. По крайней мере, один простой способ проникновения существовал в 71% компаний.

Недостатки защиты Web-приложений

В 77% случаев векторы проникновения были связаны с недостатками защиты Web-приложений. Хотя бы один такой вектор был выявлен в 86% компаний.

Web-приложение как ПО может содержать критически опасные ошибки. Приведем пример эксплуатации такой ошибки. В приложении существовала возможность загрузки документов, которые затем проверялись антивирусом, а путь к антивирусу администратор мог указать самостоятельно в файле конфигурации. Этот путь был заменен на команду загрузки скрипта на языке Perl. Когда от имени обычного пользователя был загружен документ, вместо запуска антивирусной проверки приложение скопировало скрипт на сервер. Затем путь к антивирусу был заменен на команду для выполнения скрипта. После загрузки очередного документа было установлено со-



[1] Атака — действия нарушителя, направленные на эксплуатацию недостатка защищенности. Атака может состоять из нескольких последовательных шагов. Шаг атаки — действие нарушителя, которое позволяет ему получить информацию или привилегии, необходимые для дальнейшего развития атаки.

[2] Вектор проникновения (атаки) — это способ преодоления сетевого периметра с помощью эксплуатации недостатков защищенности.

Тестирование программы может эффективно продемонстрировать наличие ошибок, но безнадежно неадекватно для демонстрации их отсутствия.
Эдсгер Вибе Дейкстра

единение с сервером и получена возможность выполнять произвольные команды ОС.

Остальные способы проникновения заключались главным образом в подборе учетных данных для доступа к различным сервисам на сетевом периметре, в том числе к СУБД и службам удаленного доступа.

Рекомендации. Следует регулярно проводить анализ защищенности Web-приложений. Тестирование на проникновение проводится методом черного ящика, поэтому могут быть выявлены не все недостатки. Самым эффективным методом проверки является анализ исходного кода: он позволяет найти наибольшее число ошибок. На устранение ошибок разработчикам может потребоваться значительное время. Кроме того, уязвимости выявляются не только в Web-приложениях собственной разработки, но и в решениях сторонних производителей. И пока производитель не выпустит патч, приложение будет оставаться уязвимым. Для защиты сетевого периметра рекомендуется применять межсетевой экран уровня приложений, который предотвращает эксплуатацию уязвимостей.

Подбор учетных данных

Атака на ресурсы сетевого периметра обычно начинается с подбора учетных данных пользователей к доступным сервисам, и чаще всего этот шаг оказывается успешным.

В 25% компаний идентификаторы пользователей Web-приложений, для которых используется доменная аутентификация, были подобраны через сервис Autodiscover в ПО Microsoft Exchange Client Access Server путем атаки по времени. Если идентификатор существует в системе, то при попытке авторизации в Web-приложении время ответа сервера не превышает порогового значения, как правило, это 2 секунды (пороговое значение может меняться от системы к системе). Если такого идентификатора в системе не существует, то время ответа сервера составит не больше 2 секунд. Исправления для этого недостатка нет, производитель не считает его опасным и рекомендует использовать надежные пароли, но мы показали, что его могут активно применять в атаках, поэтому следует обратить внимание на риск компрометации учетных записей.

Если злоумышленник подобрал пароль хотя бы для одной доменной учетной записи, он может узнать идентификаторы остальных пользователей, загрузив адресную книгу, где содержится список всех адресов электронной почты сотрудников организации. В одной из организаций, где проводилось тестирование уровня защищенности, таким образом удалось получить более 9 тыс. адресов электронной почты.

Простые и словарные пароли пользователей стали основными недостатками защиты на сетевом периметре. Одним из самых популярных оказался пароль формата [МесяцГод] в латинской раскладке, например Ctynz, hm2019 или Fduecn2019. Такие пароли встречались в каждой третьей компании, а в одной организации они были подобраны для более чем 600 пользователей.

Подобрав учетную запись пользователя домена, злоумышленник получает возможность подключиться к службам удаленного доступа, например, к службам удаленного рабочего стола (RDS). В одном из тестирований пользователю был доступен ограниченный набор программ, в том числе приложение 2 ГИС. Используя вызов справки в 2 ГИС, пентестеры получили доступ к процессу Windows Explorer и командной строке на этом узле и смогли выполнять произвольные команды ОС.

Каждый третий вектор проникновения состоял всего из двух действий — подбора учетной записи администратора Web-приложения или СУБД и последующего выполнения кода с помощью встроенных функций ПО. Например, в СУБД PostgreSQL существует легитимная функциональность для выполнения команд ОС с помощью создания новых таблиц, при этом пароль postgres входит в пятерку самых распространенных.

В ходе одного из пентестов специалисты обнаружили, что любому пользователю Internet доступен для подключения Web-интерфейс управления межсетевым экраном pfSense. Для доступа к нему использовалась учетная запись по умолчанию с паролем pfsense. Встроенные функции Web-интерфейса позволяли выполнять команды ОС на сервере.

Рекомендации. Убедитесь в том, что открытые для подключения интерфейсы действительно должны быть доступны всем Internet-пользователям. Регулярно проводите инвентаризацию ресурсов, доступных для подключения из Internet. Откажитесь от использования простых и словарных паролей, разработайте строгие правила для корпоративной парольной политики и контролируйте их выполнение.

Уязвимости в ПО

Для преодоления сетевого периметра широко эксплуатировались известные уязвимости в популярном ПО. Кроме того, за время работ были найдены шесть уязвимостей нулевого дня[3], которые позволяют удаленно выполнить произвольный код. Известные недостатки безопасности ПО помогли проникнуть в локальную сеть 39% компаний, а уязвимости нулевого дня — в сеть 14% компаний.

[2] Уязвимости нулевого дня — термин, обозначающий ранее неизвестные уязвимости в ПО, против которых еще не разработаны защитные механизмы.

Рекомендации.

Своевременно устанавливайте обновления безопасности для ОС и последние версии прикладного ПО. Обеспечивайте регулярный контроль появления ПО с известными уязвимостями на периметре корпоративной сети.

Основные угрозы

Целью злоумышленника может быть не только доступ к локальной сети, во время атаки он может осуществить и другие угрозы. Например, получить контроль над Web-приложением компании и использовать его для распространения вредоносного ПО, проведения атак на клиентов либо нарушить работу сайта. Компрометация учетных записей сотрудников опасна тем, что злоумышленник может получить доступ к ресурсам, использующим доменную аутентификацию, в первую очередь к электронной почте. Злоумышленник сможет читать конфиденциальную переписку и отправлять любые письма от лица сотрудников компании, включая ее руководителей. Письма от доверенных лиц не вызывают подозрений у получателей, поэтому такой метод атаки используется для мошенничества, распространения вредоносного ПО и атак на другие компании.

Выводы

Проникнуть в инфраструктуру большинства компаний может даже низкоквалифицированный хакер, поскольку векторы атак основаны на эксплуатации известных недостатков безопасности.

Самым уязвимым компонентом на сетевом периметре являются Web-приложения. Необходимо регулярно проводить анализ их защищенности. Наиболее эффективным является метод белого ящика, то есть анализ исходного кода. Уязвимости, позволяющие проникнуть во внутреннюю сеть, встречаются как в приложениях собственной разработки, так и в решениях известных производителей, а для их исправления требуется время, в течение которого приложение остается небезопасным. Для превентивной защиты Web-приложений рекомендуется использовать межсетевой экран уровня приложений (web application firewall, WAF), который позволяет предотвратить эксплуатацию существующих уязвимостей, даже если они еще не были обнаружены. Обычно компании устанавливают WAF только на отдельные сайты. Мы рекомендуем учитывать, что с его помощью можно защитить и многие системы удаленного доступа. Например, при правильно установленном WAF нарушитель не смог бы эксплуатировать уязвимость CVE-2019–19781 в популярном сейчас Citrix Gateway даже до появления патча.

Рекомендуется регулярно проводить тестирование на проникновение, чтобы на практике оценивать существующие меры обеспечения ИБ. Тестирование на проникновение с проверкой возможности реализации бизнес-рисков позволит максимально эффективно выстроить систему защиты.

Килюшева Екатерина Дмитриевна *– руководитель исследовательской группы отдела аналитики информационной безопасности Positive Technologies.*
Контактный телефон (495) 744-01-44.
Http:// www.ptsecurity.com/ru-ru

Транзас и Морской УТЦ ГУМРФ им. адмирала С.О. Макарова запустили дистанционное обучение моряков на облачных тренажерах

Компания «Транзас» (входит в группу компаний Wärtsilä) реализовала пилотный проект по дистанционному обучению моряков с применением облачных технологий. Первым российским участником проекта стал Морской учебно-тренажерный центр Государственного университета морского и речного флота им. адмирала С. О. Макарова.

Во время ограничительных мер, спровоцированных пандемией коронавируса, возник закономерный запрос на дистанционное обучение в морских образовательных организациях и учебно-тренажерных центрах. Именно поэтому было принято решение о проведении пилотного тестирования разработанной «Транзасом» облачной платформы для дистанционного обучения слушателей Морского УТЦ ГУМРФ им. адмирала С. О. Макарова.

Разработанные «Транзасом» облачные тренажеры обеспечивают групповой дистанционный доступ к рабочим станциям инструкторов, упражнениям, моделям и тренажерам учебных центров через Internet. Обучение ведется с помощью традиционных пользовательских устройств — ПК, ноутбука или планшета со стандартными Internet-браузерами.

Внедрению облачных тренажеров в процесс обучения в Морском УТЦ ГУМРФ предшествовал период тестирования инструкторами центра. После учета замечаний разработчиками «Транзаса» сервис удаленного доступа к тренажерам был запущен в образовательный процесс. К настоящему моменту более 20 групп слушателей прошли курсы в формате вебинара с применением разработанных Морским УТЦ ГУМРФ электронных контентов курсов в системе дистанционного обучения «Фарватер» и с использованием облачных тренажеров по таким направлениям, как:

- подготовка по расширенной программе для работы на нефтяных танкерах» (повторное обучение);
- подготовка по расширенной программе для работы на танкерах-химовозах» (повторное обучение);
- использование судовых РЛС/САРП/ЭКНИС.

В период тестирования сервиса и подготовки специалистов было проведено порядка 50 сессий использования облачных тренажеров.

В рамках пилотного проекта инструкторы и обучаемые смогли получить доступ к тренажерам и контенту образовательного курса вне учебного класса через облако и управлять процессом обучения в любое удобное время. При этом работать участники обучения могли из дома, находясь на борту судна или в иной локации с помощью широкого спектра устройств на базе ОС Windows и MacOS.

Это решение позволило использовать уже имеющиеся упражнения, модели, районы и сценарии, ранее разработанные инструкторами учебного заведения для решения учебных задач на «традиционных» тренажерах центра.

Http://www.wartsila.com