



Тестирование на проникновение в организациях кредитно-финансового сектора

2020



Содержание

Об исследовании	2
Ключевые результаты	2
Векторы проникновения в локальную сеть	3
Основные угрозы ИБ для сетевого периметра компаний	4
Векторы атак для получения полного контроля над инфраструктурой внутренним нарушителем	5
Примеры известных уязвимостей ПО, выявленных в корпоративной сети банков	7
Другие интересные факты	7
Выводы	8

Г Об исследовании

В 2019 году эксперты Positive Technologies провели десятки тестирований на проникновение («пентестов») корпоративных информационных систем организаций из разных отраслей¹. *Для данного исследования были выбраны 18 проектов (8 внешних тестирований и 10 внутренних), выполненных для организаций кредитно-финансового сектора, в которых заказчики работ не вводили существенных ограничений на перечень тестируемых сетей и систем.* Различие в выборках для двух типов работ объясняется тем, что каждая компания могла проводить отдельно внешний или внутренний пентест либо и тот, и другой в комплексе.

Основной целью пентестера при проведении внешнего тестирования было проникновение из интернета в локальную корпоративную сеть организации, а при внутреннем — получение максимально возможных привилегий в корпоративной инфраструктуре (компрометация контроллеров доменов, получение привилегий администраторов доменов или леса доменов²). В отдельных пентестах руководство организации ставило задачу продемонстрировать возможность получения контроля над критически важными системами (например, системами управления банкоматами, SWIFT, АРМ КБР, рабочими станциями топ-менеджеров).

Ключевые результаты

- Внешний злоумышленник может проникнуть из интернета в локальную сеть семи из восьми протестированных компаний. Общий уровень защищенности сетевого периметра шести финансовых организаций был оценен как крайне низкий (*6 — крайне низкий, 1 — низкий; 1 — выше среднего*).
- Для проникновения во внутреннюю сеть банка в среднем требуется пять дней.
- Во всех 10 организациях, где проводился внутренний пентест, удалось получить максимальные привилегии в корпоративной инфраструктуре. Причем в семи проектах полный контроль был получен в результате продолжения успешной внешней атаки из интернета. В трех проектах стояла дополнительная цель — продемонстрировать возможность хищения денежных средств банка потенциальным злоумышленником, и во всех трех проектах удалось продемонстрировать такую возможность.
- Для получения полного контроля над инфраструктурой банка внутреннему злоумышленнику потребуется в среднем два дня.
- Общий уровень защищенности корпоративной инфраструктуры большинства финансовых организаций от внутренних атак оценивается как крайне низкий (*8 — крайне низкий, 2 — низкий*).
- В рамках трех внешних пентестов и в двух внутренних были выявлены и успешно применены шесть уязвимостей нулевого дня в известном ПО.

1. В рамках тестирования моделировались атаки внешнего и внутреннего злоумышленников на элементы корпоративной информационной системы финансовых организаций без использования социальной инженерии и уязвимостей беспроводных сетей.

2. Лес доменов — это группа деревьев доменов, которые устанавливают двусторонние доверительные отношения между доменами.

Векторы проникновения в локальную сеть

Злоумышленник может использовать различные способы проникновения в локальную сеть банков. Максимальное количество разных векторов проникновения, которые были обнаружены в рамках одного проекта — пять; минимальное — один.

В одном из банков были выявлены следы более ранних взломов на множестве ресурсов сетевого периметра. Это значит, что банк не только уязвим, а уже был атакован реальным злоумышленником и не смог выявить атаку.

Сложность векторов проникновения в банки нельзя оценить однозначно. В некоторых случаях для атаки требуется высокая квалификация хакера, как например в векторах атаки с использованием уязвимостей нулевого дня. Злоумышленник должен быть готов не только найти такую уязвимость, но и разработать эксплойт. Но в большинстве организаций наряду со сложным вектором атаки выявлялся и простой, который более вероятно выбрал бы потенциальный преступник. Высоким уровнем сложности охарактеризованы семь из всех обнаруженных векторов проникновения в локальную сеть банков, низким — восемь, средним — один.

Если рассматривать каждый вектор проникновения поэтапно, то можно оценить не только сложность реализации атаки, но и число шагов, требуемых для ее выполнения³. В среднем злоумышленнику требуется всего два шага, чтобы проникнуть в локальную сеть банка (**максимум — пять; минимум — один**).

Большинство векторов атаки (44%) основаны на эксплуатации уязвимостей веб-приложений. Во многих случаях для такой атаки потребуются обладать привилегиями пользователя на сайте (иметь личный кабинет), но из-за применения простых паролей многими пользователями эти привилегии злоумышленник может получить путем подбора. А в некоторых системах возможно просто зарегистрировать нового пользователя, используя встроенные механизмы приложения.



Рисунок 1. Доля успешных векторов проникновения в локальную сеть (по категориям)

Не все успешные попытки атак в итоге приводили к проникновению в локальную сеть, однако каждая из них могла бы принести гипотетическому злоумышленнику определенную полезную для атаки информацию, доступ к важным

3. За один этап или шаг атаки мы принимаем успешное действие нарушителя, которое позволяет ему получить информацию или привилегии необходимые для дальнейшего развития атаки. В общем случае число шагов может равняться числу различных уязвимостей, которые необходимо проэксплуатировать злоумышленнику последовательно, чтобы достичь поставленной цели.

системам банка или возможность осуществить отказ в обслуживании систем и нарушить работу некоторых бизнес-процессов. Все успешные этапы атак мы распределили на пять основных категорий. Как видим, в каждой четвертой попытке атаки были поэксплуатированы уязвимости веб-приложений, что говорит о недостаточном внимании банков к их защите.



Рисунок 2. Доля успешных атак разных типов

Использование на сетевом периметре устаревших версий ПО является серьезным риском, при этом хотя бы одна атака с использованием известного общедоступного эксплойта оказывалась успешной в ходе тестирования в каждом втором банке. Примеры использованных уязвимостей (по идентификатору CVE):

- [CVE-2018-15133](#) (уязвимость фреймворка Laravel позволяет выполнять команды на сервере веб-приложения, если злоумышленнику известен APP_KEY приложения);
- [CVE-2018-15473](#) (уязвимость ПО OpenSSH позволяет подбирать идентификаторы системных пользователей);
- [CVE-2014-9223](#) (уязвимость типа «переполнение буфера» устаревшей версии прошивки роутера Zyxel позволяет удаленно выполнить произвольный код);
- [CVE-2018-0171](#) (уязвимость ПО Smart Install для Cisco IOS позволяет удаленно выполнить произвольный код).

Одной из уязвимостей нулевого дня, которую *обнаружили эксперты Positive Technologies*, была уязвимость [CVE-2019-19781](#) в ПО Citrix Application Delivery Controller (ADC) и Citrix Gateway, которая гипотетически позволяет выполнять произвольные команды ОС на сервере и проникнуть в локальную сеть организации.

Основные угрозы ИБ для сетевого периметра компаний

Внешний злоумышленник может ставить целью не только проникновение в локальную сеть банка, но и получение контроля над сайтом банка или над конкретным сервером. Он может использовать взломанные системы для распространения вредоносного ПО и проведения других атак на клиентов банка и другие компании, используя доверительное отношение к таким ресурсам. Также злоумышленник может получить учетную запись нужного ему

сотрудника, использовать ее в других атаках. Например, он может подключиться к почтовому ящику этого сотрудника, читать его почту и отправлять письма от его имени. Такая атака наиболее опасна в случае компрометации учетных записей высокопоставленных лиц и носит название *business email compromise*.

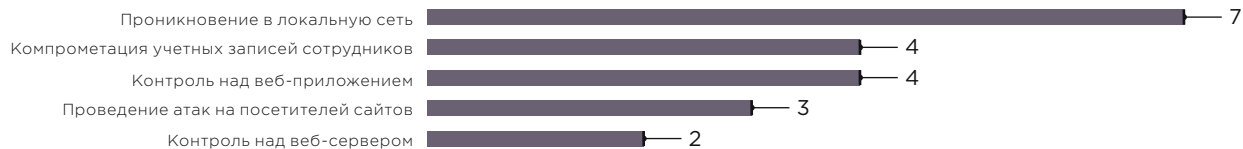


Рисунок 3. Угрозы для сетевого периметра финансовых организаций (число компаний)

Векторы атак для получения полного контроля над инфраструктурой внутренним нарушителем

В среднем на каждый банк приходится по два разных вектора атаки, позволяющих получить полный контроль над инфраструктурой. Как и в случае с внешним пентестом, такие векторы можно разделить на основные этапы (шаги). Атакующему приходится переключаться между узлами в локальной сети в поисках тех серверов, где он сможет получить учетную запись администратора домена. Поэтому вектор атак может оказаться достаточно протяженным, а в среднем состоит из восьми шагов (*минимально — два, максимально — 15*).

Большинство выявленных векторов атак были сложны в реализации, девять характеризуются высокой сложностью (*пять — средней, и еще 5 — низкой*). Для проведения сложной атаки, злоумышленнику необходимо обладать высокой квалификацией и понимать, как обойти различные системы защиты. При этом в восьми банках существовал одновременно и альтернативный способ атаки, более простой в реализации, для которого нарушителю достаточно было бы обладать базовыми навыками, использовать общедоступные инструменты и эксплойты.

Во время внутреннего тестирования на проникновение не все атаки попадают в цепочку, которая в результате приведет к получению полного контроля над инфраструктурой. При этом многие уязвимости, которые встречаются на пути к главной цели могут приводить к реализации значимых для бизнеса рисков. К примеру, может быть получен контроль над рабочей станцией высокопоставленного лица компании или доступ к базам данных, бизнес-системам и различной важной информации, утечка которой повлечет существенные репутационные потери.

В среднем на каждый банк приходилось по 19 успешных попыток атак разных типов, которые приводили к получению важной для продолжения атаки информации или необходимые привилегии в ключевых системах. Если рассмотреть наиболее распространенные из них, получается следующая картина:



Рисунок 4. Успешные атаки разных типов (число компаний)

В каждом пентесте активно использовались атаки на подбор учетных данных, а также вполне легальные действия в системах, которые позволяли получать несанкционированный доступ или нужную информацию. Например, если сделать дамп процесса lsass.exe в ОС Windows, в дальнейшем можно использовать этот дамп для восстановления учетных данных пользователей ОС атакованного узла. Также к легальным действиям можно причислять запросы к контроллеру домена, получение паролей локальных администраторов из LAPS и другие действия, предусмотренные функциональностью атакуемых систем.

В восьми из 10 банков системы антивирусной защиты, установленные на рабочих станциях и серверах, не препятствовали созданию дампов процессов или запуску специализированных утилит, таких как secretdump.

В большинстве проектов активно применялись техники атак, использующие архитектурные особенности протокола аутентификации Kerberos (например, pass-the-ticket и kerberoasting).

Недостатки сетевой безопасности выявлялись в каждом проекте, но использованы в атаке были только в двух банках из 10. Это связано с тем, что такие атаки могут нарушить сетевое взаимодействие и приостановить бизнес-процессы, поэтому атаки в большинстве проектов просто не проводились. Поэтому они не попали на диаграмму на рисунке 4 и составили незначительную долю от всех успешных атак (рисунок 5).

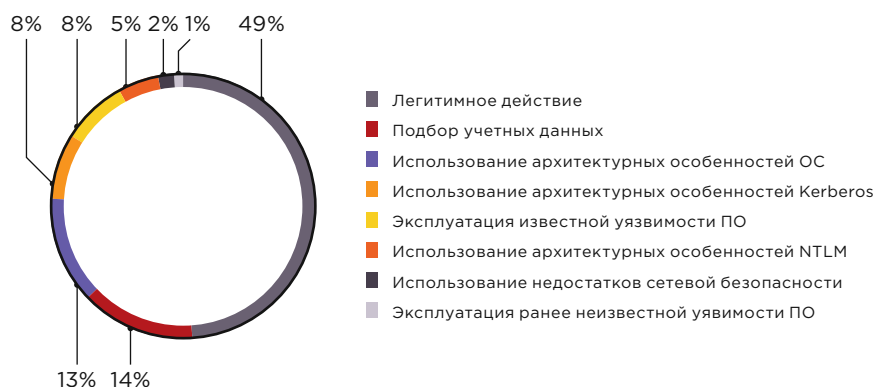


Рисунок 5. Распределение всех успешных атак по категориям (доля атак)

Успешные атаки в рамках всех проведенных внутренних пентестов распределяется по категориям следующим образом:

Из этого распределения видно, насколько много возможностей у потенциального злоумышленника по использованию легитимных действий и инструментов в атаке. Это позволяет скрыть атаку, так как действия хакера становятся почти неотличимы от повседневной работы сотрудников и систем.

Получение полного контроля над инфраструктурой банка открывает нарушителю множество возможностей для компрометации критически важных для бизнеса систем. Так, например, в ходе тестирования в разных банках, в разных банках демонстрировалась возможность получения доступа к следующим типам систем:

- банкоматам,
- рабочим станциям топ-менеджеров,
- серверам карточного процессинга,
- центрам управления антивирусной защитой.

Примеры известных уязвимостей ПО, выявленных в корпоративной сети банков

В локальной сети банков по-прежнему можно встретить множество необновленных систем, содержащих опасные уязвимости. Например, следующие:

- [CVE-2018-9276](#) (уязвимость в ПО PRTG Network Monitor позволяющая выполнить команды ОС на сервере при наличии прав администратора приложения),
- [CVE-2016-2004](#) (уязвимость в ПО HP Data Protector позволяет удаленно выполнить произвольный код);
- [CVE-2018-0171](#) (уязвимость ПО Smart Install для Cisco IOS позволяет удаленно выполнить произвольный код);
- [CVE-2019-0686](#) (уязвимость ПО Microsoft Exchange Server позволяет повысить привилегии в системе);
- [CVE-2017-10271](#) (уязвимость в ПО Oracle WebLogic Server с уязвимым компонентом WLS-WSAT позволяет удаленно выполнить произвольные команды на сервере).

Встречались и столь известные уязвимости, как рассмотренные в бюллетенях безопасности [MS17-010](#) (использовалась в атаке WannaCry) и даже [MS08-067](#), позволяющие получить полный контроль над ОС Windows.

Другие интересные факты

Во время проведения внешнего пентеста может быть полезна любая дополнительная информация о тестируемой организации и ее системах. Поэтому на этапе разведки, когда собирается информация из общедоступных источников, анализируются в том числе такие площадки как социальные сети, базы утечек, ресурсы для публикации проектов с открытым исходным кодом, и другие. В частности, в ходе проведенных тестирований были обнаружены и использованы следующие типы данных о банках:

- файлы конфигурации систем,
- учетные данные для доступа СУБД,
- IP-адреса банковских систем,
- персональные данные сотрудников и клиентов,
- значения ключа APP_KEY приложения (используется в атаке на фреймворк Laravel),
- листинги директорий.

Не меньший интерес представляют и подобранные простые пароли пользователей. Потенциальный злоумышленник может составлять специальные словари из подобранных значений и применять их для атак на другие ресурсы компании. Ведь пользователи могут использовать одинаковые пароли для разных систем, что повышает шанс успешной атаки.

Подавляющее большинство успешно подобранных в ходе пентестов паролей были составлены предсказуемым образом. Если рассмотреть пароли, подобранные на сетевом периметре банков, то половина из них была различными комбинациями месяца или времени года с цифрами, обозначающими год (например, Fduesn2019, Зима2019). Часто такие пароли используются сотрудниками для доменной учетной записи и подключения к корпоративным

ресурсам. А на втором месте по распространенности оказались пароли типа 123456, 1qaz!QAZ, Qwerty123, которые состояются из близкорасположенных клавиш на клавиатуре. Пользователи часто пытаются усложнить пароль за счет изменения раскладки клавиатуры при наборе слова, однако пентестеры в курсе такой хитрости и учитывают ее в используемых для подбора словарях.

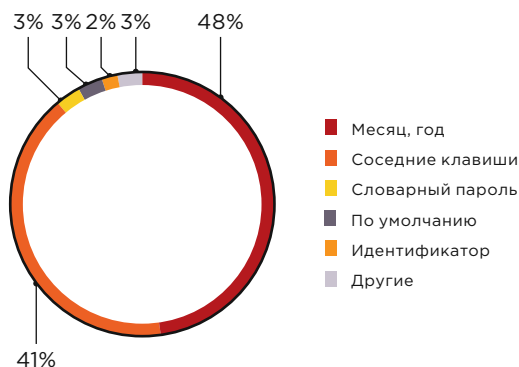


Рисунок 6. Подобранные пароли на сетевом периметре по категориям (доля паролей)

Во внутренней инфраструктуре банков картина похожа. В каждом втором банке использовались различные словарные комбинации для паролей (например, AB1234567, admin123) или пароли, состоящие из соседних клавиш (такие как !QAZ2wsx). Причем в рамках одного домена может быть множество (доходит до нескольких сотен) пользователей с одинаковым паролем. К примеру, в одном из банков было подобрано более 500 учетных записей с паролем qwerty123 для доменных учетных записей. Это может происходить, когда для вновь созданных учетных записей используется один и тот же пароль, который сотрудник должен поменять при первом входе в систему. Однако в данном примере учетные записи оказались активны. Если наша догадка верна, то, вероятно, пользователи их не сменили, либо установили сами при последующей смене учетных данных.

Выводы

Уровень защищенности корпоративной инфраструктуры банков от целенаправленной атаки со стороны как внешнего, так и внутреннего злоумышленника, достаточно низкий. В компаниях, в которых не обеспечены эффективный мониторинг событий ИБ и реагирование на выявленные инциденты, нарушитель может не только получить контроль над ключевыми системами, но и проводить атаки, нацеленные на хищение денег. Поэтому мы рекомендуем регулярно проводить тестирование на проникновение и тренинги сотрудников ИБ в рамках «red teaming». Это позволит обнаруживать и своевременно устранять потенциальные векторы атак на критически важные ресурсы, а также отработать действия служб ИБ в случае выявления реально кибератаки, проверить эффективность используемых средств защиты и мониторинга.

О компании

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.