



# Тестирование корпоративных информационных систем на проникновение

Итоги внешних пентестов — 2020



# Содержание

Что такое тестирование на проникновение	3
Пентест и пентестер	3
Зачем проводят пентест	4
Кто заказывает пентесты	4
Что дает пентест бизнесу	5
Об исследовании	6
Ключевые цифры	6
Как мы проникали во внутренние сети	7
Основные угрозы	16
Выводы и рекомендации	17

# Что такое тестирование на проникновение

## Пентест и пентестер

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 ИБ ищут уязвимости в системах определенной компании и пытаются провести атаки в обход установленных средств защиты.

Когда тестирование проводится из внешних сетей (например, из интернета), 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 пентест. 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.

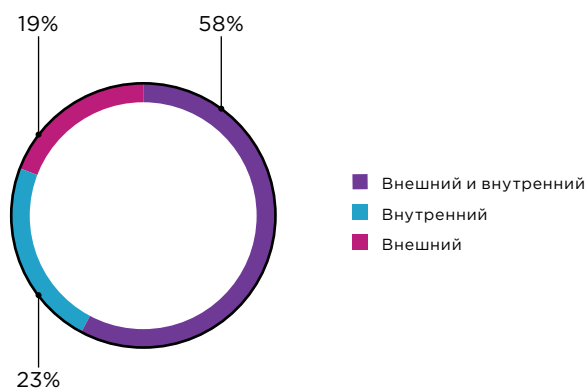


Рисунок 1. Типы пентестов, которые проводились в 2019 году

Считается, что 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, соответственно, 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.

## Зачем проводят пентест

Цель 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; оно не является основной задачей. Хакеры 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).

## Кто заказывает пентесты

Пентест может быть полезен для любой организации, независимо от сферы деятельности. Однако работы стоит проводить, когда в организации 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 высок. Особенно важно проводить тестирование на проникновение крупным компаниям с распределенной инфраструктурой, поскольку трудно обеспечить безопасность достаточно сложной системы без проверки эффективности ее защиты.

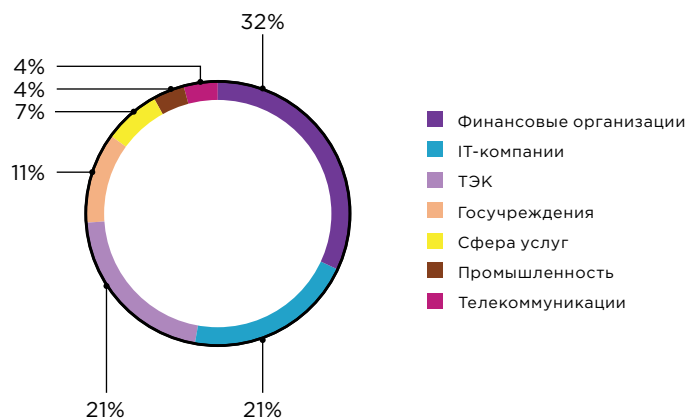


Рисунок 2. Распределение протестированных компаний по отраслям

## 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, в свою очередь, 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 информационной безопасности, 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.

## Об исследовании

В отчете представлены результаты проектов по анализу защищенности корпоративных информационных систем от внешних нарушителей, выполненных в 2019 году специалистами Positive Technologies. Документ содержит обзор наиболее распространенных недостатков безопасности и методов атак, а также 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. Мы учитывали только наиболее информативные проекты, чтобы получить объективные результаты. Проекты, в которых накладывались существенные ограничения на действия экспертов или которые проводились на ограниченном количестве узлов, не вошли в выборку, поскольку не отражают реального состояния защищенности систем.

Мы будем рассматривать только атаки на инфраструктуру, в отчет не входят атаки методами социальной инженерии, а также атаки через беспроводные сети. Результаты работ по внутреннему тестированию на проникновение мы опубликуем в отдельном документе.

## Ключевые цифры

- Преодолеть сетевой периметр и получить доступ к ресурсам локальной сети удалось в 93% компаний.
- В каждой шестой компании были обнаружены следы атак злоумышленников. Это означает, что инфраструктура уже могла быть под контролем хакеров.
- На проникновение в локальную сеть требовалось в среднем четыре дня, а минимум — 30 минут.
- В 71% компаний проникнуть во внутреннюю сеть может даже низкоквалифицированный хакер.
- Три четверти векторов проникновения (77%) связаны с недостаточной защитой веб-приложений, и хотя бы один такой вектор был выявлен в 86% компаний.

## Как мы проникали во внутренние сети

**Вектор проникновения** — это способ преодоления сетевого периметра с помощью эксплуатации недостатков защищенности

В 2019 году в ходе внешних пентестов нам удалось получить доступ к локальным сетям 93% организаций. Чаще всего существовало несколько способов преодолеть сетевой периметр, в среднем в одной компании выявлялось два вектора проникновения. Максимальное число векторов проникновения, выявленных в одном проекте, — 13.



В каждой шестой компании были обнаружены следы атак злоумышленников — выявлены веб-шеллы на ресурсах сетевого периметра, вредоносные ссылки на официальных сайтах или валидные учетные записи в публичных базах утечек. Это говорит о том, что инфраструктура уже могла быть под контролем хакеров.

### От 30 минут до 10 дней

требуется  
на проникновение  
в локальную сеть  
компании

На проникновение в локальную сеть требовалось в среднем четыре дня, а минимум — 30 минут. В большинстве случаев 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.

### В 68% компаний

злоумышленник может  
получить доступ  
к внутренней сети  
не более чем за два шага

**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



Рисунок 3. Минимальное число шагов, необходимое для проникновения в локальную сеть (доли компаний)

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

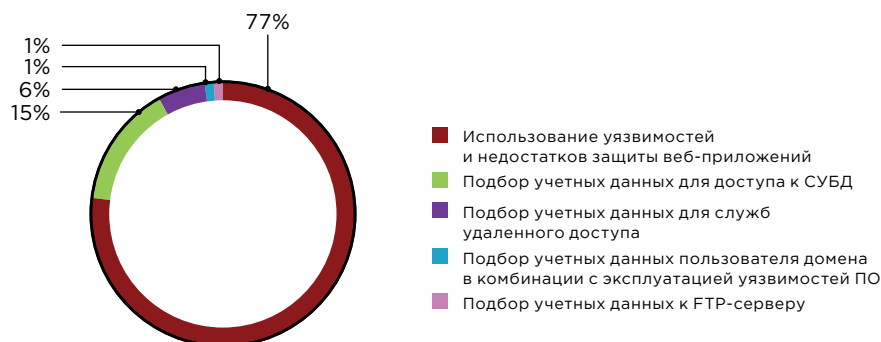


Рисунок 4. Векторы проникновения в локальную сеть (доли векторов)

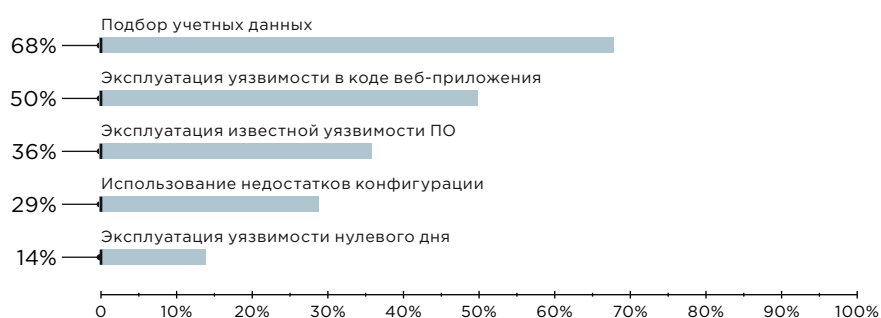


Рисунок 5. Атаки на веб-приложения, которые привели к проникновению в локальную сеть (доли компаний)

## Рекомендации

Следует регулярно проводить анализ защищенности веб-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 количество ошибок. На устранение ошибок разработчикам может потребоваться значительное время, кроме того, уязвимости выявляются не только в веб-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.

Не каждая атака ведет к проникновению во внутреннюю сеть, но при этом злоумышленник может получить доступ к другим важным ресурсам или нарушить работу бизнес-систем. На диаграмме ниже приведено распределение всех успешных атак по категориям. Наибольшее количество среди них было направлено на подбор учетных данных и на эксплуатацию уязвимостей веб-приложений.



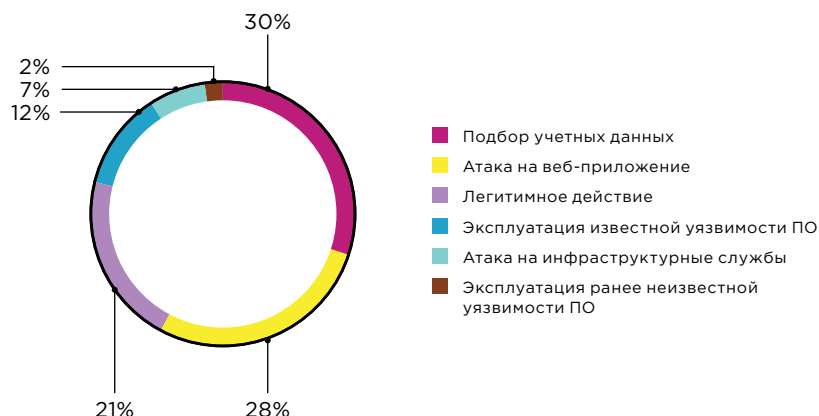


Рисунок 6. Успешные атаки

На следующей диаграмме отображена оценка опасности выявленных уязвимостей. Каждой уязвимости присваивается уровень риска (критический, высокий, средний или низкий), который рассчитывается в соответствии с системой CVSS 3.1. Необходимо учитывать, что работы по тестированию на проникновение проводятся методом черного ящика, поэтому выявить все уязвимости, существующие в системе, невозможно, более того, это не является целью. Цель пентеста заключается в получении объективной оценки уровня защищенности системы от атак со стороны внешних нарушителей.



Рисунок 7. Максимальный уровень риска уязвимостей (доли компаний)

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 веб-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 веб-приложении время ответа сервера не превышает порогового значения, как правило это две секунды (пороговое значение может меняться от системы к системе). Если такого идентификатора в системе не существует, то время ответа сервера составит более двух 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 Offline Address Book, где содержится список всех адресов электронной почты сотрудников организации. В одной из организаций, где проводилось тестирование, таким образом удалось получить более 9000 адресов электронной почты.

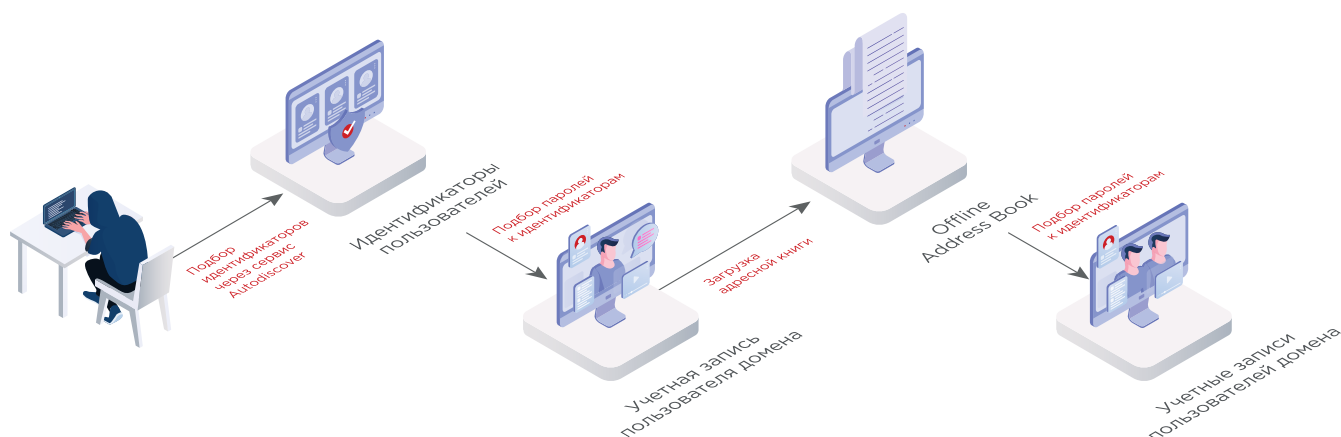


Рисунок 8. Получение учетных записей пользователей домена

Для получения идентификаторов использовалась также уязвимость [CVE-2018-15473](#) в устаревшей версии OpenSSH, причем в одном проекте так были выявлены сразу два вектора проникновения.

Простые и словарные пароли пользователей стали основными недостатками защиты на сетевом периметре. Одним из самых популярных оказался пароль формата [МесяцГод] в латинской раскладке, например Stynz,hm2019 или Fduesn2019. Такие пароли встречались в каждой третьей компании, а в одной организации они были подобраны для более чем 600 пользователей.

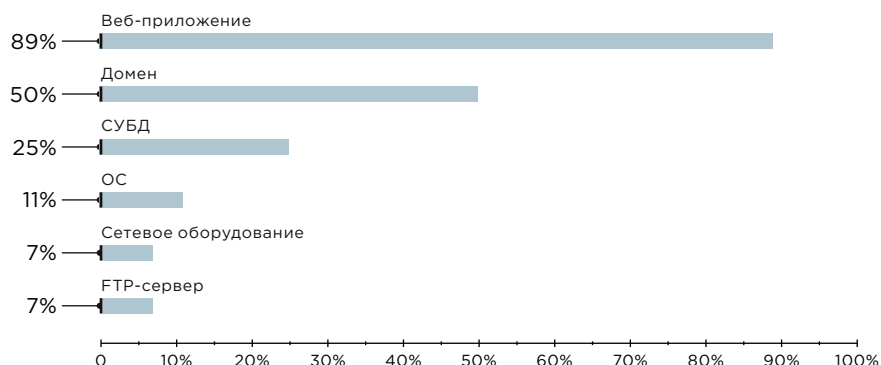


Рисунок 9. Где обнаружены ненадежные пароли (доли компаний)

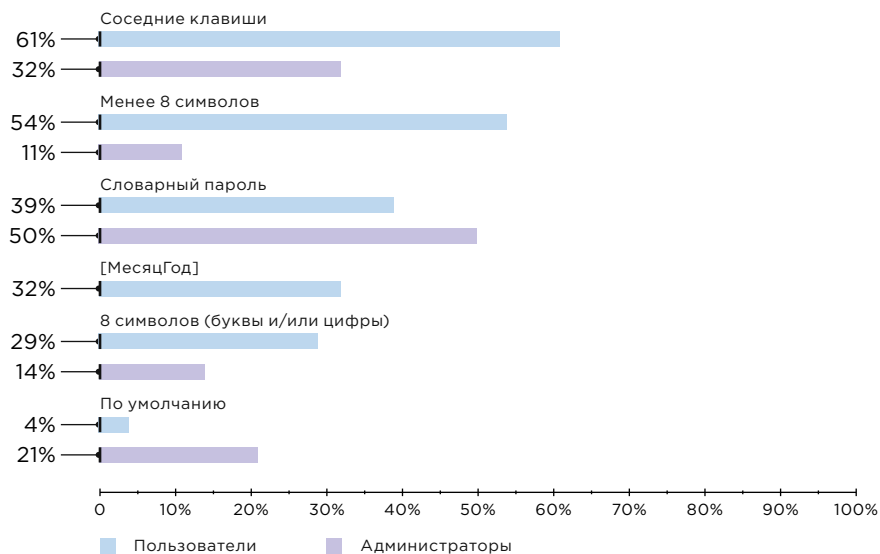


Рисунок 10. Самые распространенные пароли (доли компаний)

### Пример атаки

**Категория:** подбор учетных данных для служб удаленного доступа

**Сложность:** низкая

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

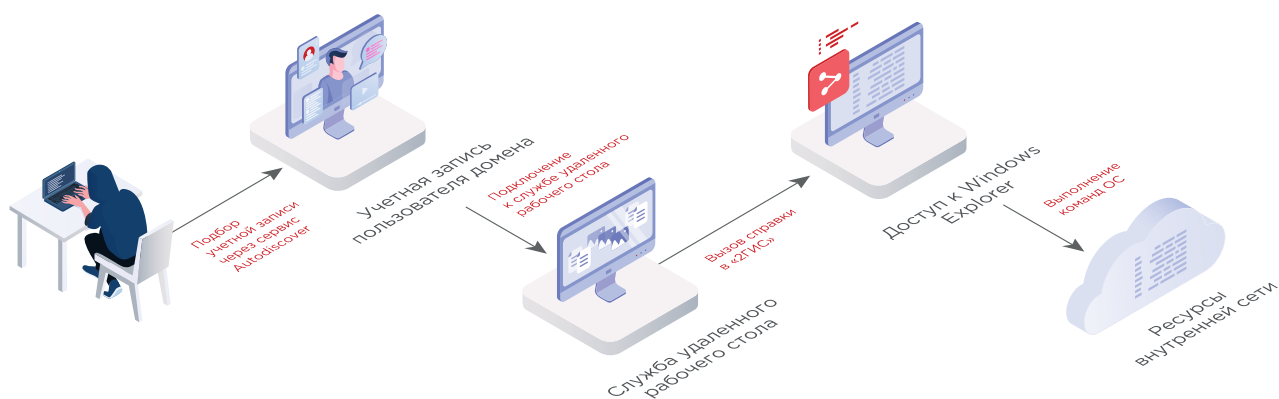


Рисунок 11. Вектор проникновения через подключение к службе удаленного рабочего стола

Каждый третий вектор проникновения состоял всего из двух действий — подбора учетной записи администратора веб-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.

### Пример атаки

**Категория:** подбор учетных данных

**ПО:** pfSense

**Сложность:** низкая

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

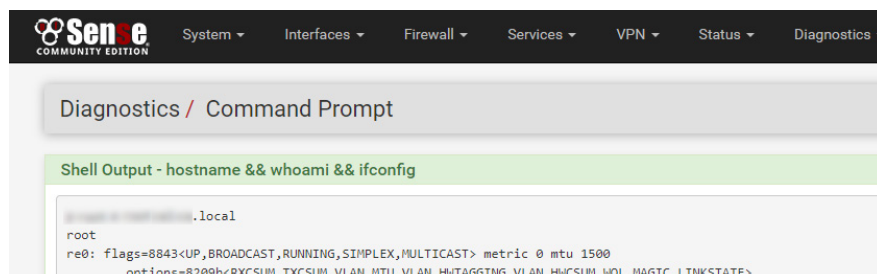


Рисунок 12. Выполнение команд ОС в веб-интерфейсе администрирования межсетевого экрана

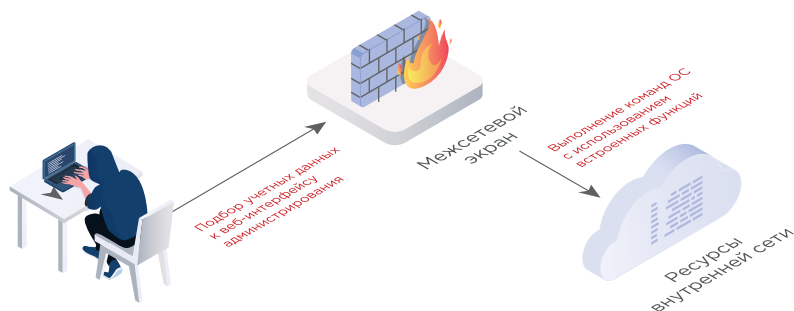


Рисунок 13. Вектор проникновения

## Рекомендации

Убедиться в том, что открытые для подключения интерфейсы действительно должны быть доступны всем интернет-пользователям. Регулярно проводить инвентаризацию ресурсов, доступных для подключения из интернета.

Отказаться от использования простых и словарных паролей, разработать строгие правила для корпоративной парольной политики и контролировать их выполнение.

Веб-приложение может не содержать легитимной функциональности для выполнения команд, однако при его разработке или конфигурации могут быть допущены критически опасные ошибки. Приведем пример эксплуатации такой ошибки.



### Пример атаки

#### Категория:

эксплуатация уязвимости  
в веб-приложении

**Сложность:** низкая

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. После того как 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 соединение с сервером и получена возможность выполнять произвольные команды ОС.

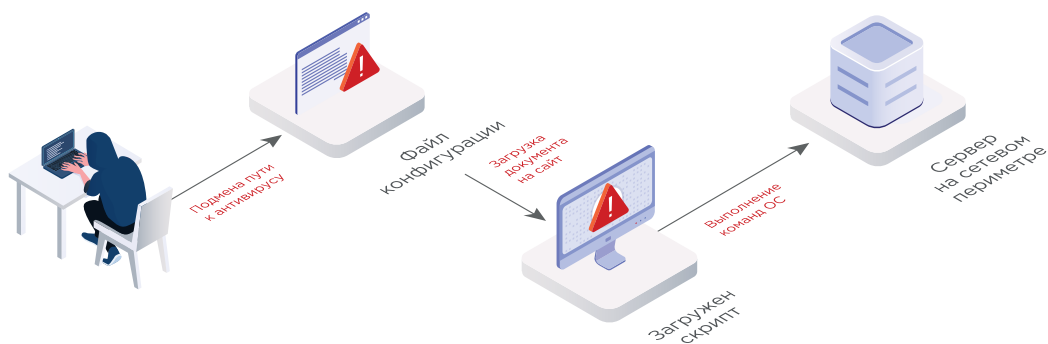


Рисунок 14. Эксплуатация уязвимости веб-приложения

Для преодоления сетевого периметра широко эксплуатировались уязвимости в ПО, например [CVE-2018-15133](#) в фреймворке Laravel, [CVE-2018-8284](#) в .NET Framework, [CVE-2017-10271](#) в Oracle WebLogic Server. Кроме того, за время работ были найдены шесть уязвимостей нулевого дня, которые позволяют удаленно выполнить произвольный код, в том числе [CVE-2019-19781](#) в Citrix Application Delivery Controller (ADC) и Citrix Gateway. Уязвимости нулевого дня были выявлены и в других популярных продуктах известных производителей, однако они пока не исправлены, и мы не можем сообщать подробности.

В начале 2020 года наши эксперты обнаружили две опасные уязвимости нулевого дня в межсетевом экране Cisco ASA: [CVE-2020-3187](#) и [CVE-2020-3259](#). Их эксплуатация может привести к отключению VPN в Cisco ASA или к тому, что злоумышленник получит доступ во внутреннюю сеть организации. Компания Cisco уже выпустила обновления, устраняющие эти уязвимости, мы рекомендуем как можно скорее установить актуальные версии.

Известные недостатки безопасности ПО помогли проникнуть в локальную сеть 39% компаний, а уязвимости нулевого дня — в сеть 14% компаний.

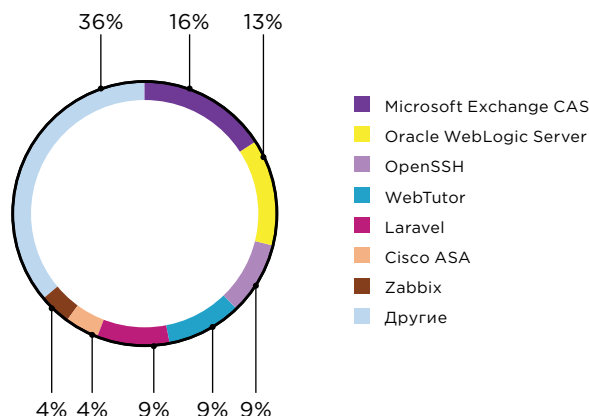


Рисунок 15. ПО, в котором были выявлены уязвимости (доли уязвимостей)

### Пример атаки

**Категория:** эксплуатация известной уязвимости ПО

**ПО:** Laravel

**Сложность:** низкая

Приведем пример проникновения в локальную сеть посредством эксплуатации известной уязвимости фреймворка Laravel. Во время тестирования наши эксперты обнаружили, что любой внешний злоумышленник может получить параметры конфигурации среды веб-приложения, в том числе значение ключа приложения APP\_KEY.

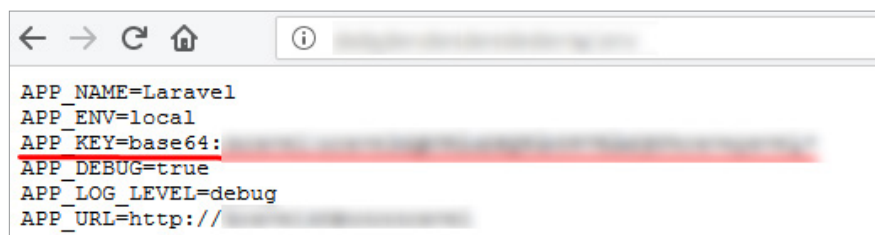


Рисунок 16. Раскрытие конфигурационной информации веб-приложения

Для работы веб-приложения использовался PHP-фреймворк Laravel устаревшей версии, которая содержит уязвимость «Удаленное выполнение произвольного кода» (CVE-2018-15133). Для эксплуатации уязвимости требуется лишь значение ключа приложения APP\_KEY, которое уже известно. С помощью утилиты PHPGGC была подготовлена полезная нагрузка, при выполнении которой с атакуемого узла устанавливается соединение на внешний узел. Сгенерированная полезная нагрузка была зашифрована при помощи ключа APP\_KEY и специальной общедоступной утилиты, в результате было получено содержимое HTTP-заголовка X-XSRF-TOKEN, необходимого для проведения атаки. Эксплуатация уязвимости позволила получить доступ к локальной сети.

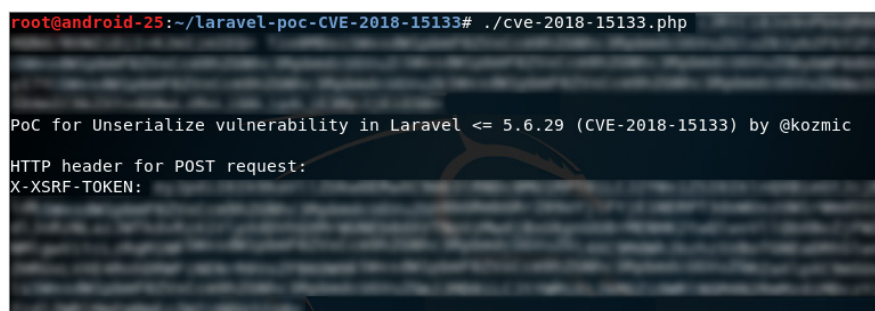


Рисунок 17. Создание HTTP-заголовка для эксплуатации уязвимости

## Пример атаки

### Категория:

эксплуатация известной уязвимости ПО

ПО: Microsoft Outlook

Сложность: низкая

Рассмотрим вектор проникновения, в котором эксплуатируется уязвимость в устаревшей версии Microsoft Outlook. Для проведения атаки необходима валидная учетная запись пользователя домена (как ее получить, мы уже знаем).

Microsoft Outlook использует сервисы MAPI/HTTP или RPC/HTTP для получения электронных писем, их отправки и хранения параметров обработки почты. Утилита Ruler позволяет удаленно взаимодействовать с сервером Microsoft Exchange через эти сервисы. Если на рабочих станциях пользователей используются устаревшие версии Microsoft Outlook, злоумышленник, обладающий учетной записью пользователя домена, может создавать собственные правила обработки электронных писем, которые синхронизируются с Microsoft Outlook на стороне клиента. Эти правила могут включать запуск скриптов или открытие форм, выполняющих код на языке VBA, при определенных условиях, например при получении письма с заранее известной темой.

В ходе тестирования на проникновение наши специалисты с помощью утилиты Ruler обнаружили, что на сервере Microsoft Exchange, для доступа к которому были подобраны учетные записи доменных пользователей, доступны сервисы MAPI/HTTP и RPC/HTTP.

```
$ ./ruler-linux64 --domain --username --password
--email check
[+] Retrieving MAPI/HTTP info
[+] Binding to RPC
[+] Looks like we are good to go!
```

Рисунок 18. Проверка доступности сервисов с помощью утилиты Ruler

Одному из пользователей было добавлено правило обработки электронной почты, которое должно при получении письма с определенной темой загружать файл с расширением .bat с внешнего сервера и запускать его.

Логика обработки UNC-путей в Windows такова, что вначале будет выполнено обращение к удаленному ресурсу по протоколу SMB и затем, в случае возникновения ошибки, по протоколу WebDAV. Таким образом, после отправки электронного письма с заданной темой было установлено соединение по протоколу WebDAV, загружен и запущен .bat-файл на рабочей станции пользователя. Этот файл, в свою очередь, загружает специализированное ПО на языке PowerShell, которое создает соединение с сервером пентестеров. В результате была получена возможность выполнять команды ОС с привилегиями пользователя в локальной сети компании.

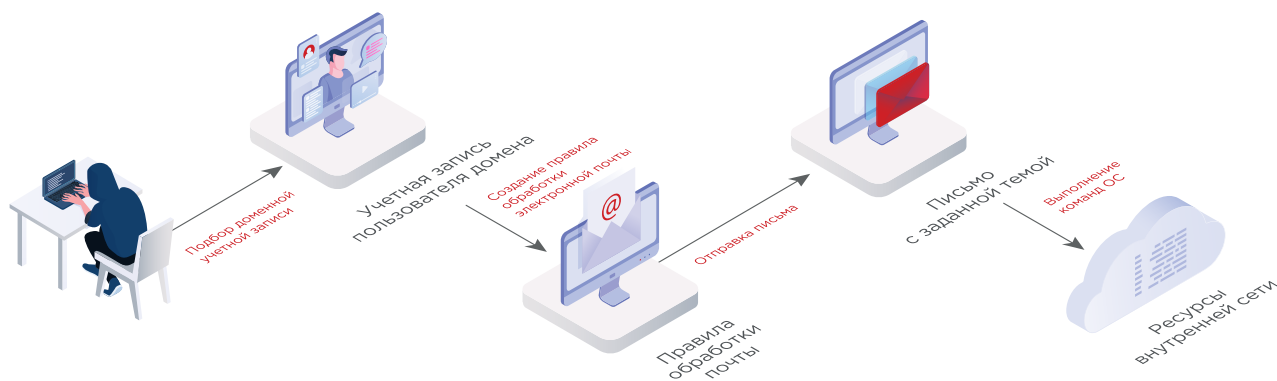


Рисунок 19. Вектор проникновения через устаревшую версию Microsoft Outlook

## Рекомендации

Своевременно устанавливать обновления безопасности для ОС и последние версии прикладного ПО. Обеспечить 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 веб-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. Отметим, что в рамках тестирования на проникновения мы лишь демонстрируем недостатки защиты, которые позволяют проводить такие атаки.

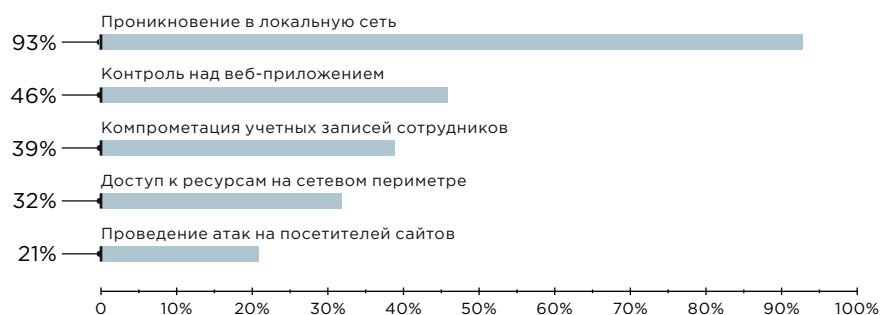


Рисунок 20. Основные угрозы на сетевом периметре (доля компаний)



## Выводы и рекомендации

Проникнуть в инфраструктуру большинства компаний может даже низко-квалифицированный хакер, поскольку векторы атак основаны на эксплуатации известных недостатков безопасности. В первую очередь, для защиты сетевого периметра необходимо соблюдать общие принципы обеспечения информационной безопасности. Рекомендации по защите от наиболее распространенных векторов проникновения приведены в исследовании.

Самым уязвимым компонентом на сетевом периметре являются веб-приложения. Необходимо регулярно проводить анализ их защищенности. Наиболее эффективным методом 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 веб-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, однако 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 Citrix Gateway даже до появления патча.

Важно на практике оценивать, как работают все принимаемые меры защиты, поэтому тестирование на проникновение следует проводить регулярно, чтобы выявлять и устранять новые векторы проникновения в систему. Тестирование на проникновение с проверкой возможности реализации ключевых бизнес-рисков компании в результате кибератак позволит выстроить защиту более эффективно.

---

### О компании

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

Positive Technologies уже 18 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях ([Facebook](#), [ВКонтакте](#), [Twitter](#)), а также в разделе «Новости» на сайте [ptsecurity.com](#).