АНАЛИТИЧЕСКИЙ ОБЗОР

Киберучения в формате Red Teaming. Имитация целевых атак и регулярное противодействие им.

GROUP-IB

СОДЕРЖАНИЕ

01 ВВЕДЕНИЕ

Организации регулярно сталкиваются с кибератаками разной сложности: от технических подходов до социальной инженерии. Для защиты от подобных угроз они задействуют лучшие средства и оборонительные тактики.

Однако злоумышленники также применяют самый передовой инструментарий и новейшее вредоносное ПО, противодействовать которым не всегда готовы даже наиболее защищенные ИТ-инфраструктуры и системы. Недостаток опыта активного реагирования на инциденты зачастую приводит к тому, что компания становится жертвой кибератаки и главным героем СМИ.

Для усиления кибербезопасности на рынке существует множество услуг по проверке защищенности: анализ защищенности систем и приложений, тестирование на проникновение и оценка осведомленности персонала в вопросах информационной безопасности. Несмотря на эффективность данных мер по проверке безопасности, они нацелены на точечную оценку в течение короткого промежутка времени.

Ежегодно количество инцидентов информационной безопасности растет более чем на 10%, поэтому организациям необходимо быть готовыми к реальным атакам, которые не ограничены какими-либо рамками. В связи с изменением ландшафта киберугроз появились и новые типы риска, которые трудно выявить с помощью традиционных способов анализа защищенности.

Самым реалистичным и продвинутым подходом к тестированию безопасности является Red Teaming — непрерывная оценка защищённости систем, готовности специалистов по реагированию на инциденты и устойчивости инфраструктуры к новым видам атак, в том числе составных и продолжительных (APT).

02

ЧТО ТАКОЕ RED TEAMING?

Red Teaming — комплексный и максимально реалистичный способ проверки способности организации к отражению сложных кибератак с использованием продвинутых методов и инструментов из арсенала хакерских группировок

Основная цель данного упражнения не только выявить потенциально слабые стороны, которые не были обнаружены с помощью стандартных методологий тестирования, но и оценить способность организации предотвращать, обнаруживать и реагировать на кибератаки.

В связи с этим служба безопасности Заказчика (Blue Team) не информируется о начале работ, чтобы Красная команда (Red Team) могла смоделировать действия реальных атакующих на основе специального анализа угроз и оценить возможность взлома инфраструктуры контролируемым и эффективным способом.

Объекты исследования:

Технологии
сеть, приложения и т.д.

Люди
сотрудники и партнеры

Материальные активы
офисы и склады

Red Teaming позволит службе информационной безопасности Заказчика эффективно проработать проблемные моменты в ключевых элементах организации — таких как люди, бизнес-процессы, технологии и связанные с ними точки пересечения.

Основные сценарии Red Teaming

Сценарий Red Teaming исследования индивидуален для каждого Заказчика и зависит от поставленных целей. Наиболее часто используемые сценарии включают:

- захват леса AD (AD Forest takeover);
- «кражу» чувствительных данных клиента;
- доступ к устройству топ-менеджмента;
- «кражу» интеллектуальной собственности.

Преимущества Red Teaming

- никак не ограничен по времени воздействия;
- максимально эффективен для компаний со «зрелым» уровнем информационной безопасности;
- сосредоточен на достижении конкретно поставленных целей, будь то получение доступа к сетевым узлам или информации любыми доступными способами.

Полномасштабные киберучения дают ответы на следующие вопросы:

01 | Как средства безопасности организации защищают важные данные?

02 | Корректно ли настроена система оповещения и мониторинга?

03 | Насколько внутренняя команда безопасности готова противодействовать атаке высококвалифицированного злоумышленника?

04 | Какие возможности открываются злоумышленнику во внутренней инфраструктуре, если пользователь скомпрометирован?

Исследование максимально приближено к поведению реального злоумышленника, чтобы наглядно продемонстрировать возможные сценарии хакерских атак и одновременно разработать эффективную защиту информационных систем.

По результатам Red Teaming организации удастся оценить риск, связанный с APT (Advanced Persistent Threat).

03 RED TEAMING VS.
Penetration Testing

Несмотря на то, что в Red Teaming и Penetration Testing применяются схожие инструменты кибератаки, цели и результаты обоих исследований сильно отличаются.

Red Teaming

В процессе Red Teaming имитируются реальные и целенаправленные атаки на всю организацию. Преимущество такого подхода заключается в непрерывном исследовании информационных систем для достижения целей. Такая глубокая проверка дает исчерпывающее понимание того, насколько защищена инфраструктура, осведомлены сотрудники и эффективны внутренние процессы организации, когда она подвергается реальной атаке.

Penetration Testing

В ходе данного исследования специалист по тестированию на проникновение пытается проэксплуатировать обнаруженную уязвимость и повысить свои привилегии, чтобы понять возможный риск. Данное тестирование не проверяет готовность к обнаружению и реагированию на инциденты информационной безопасности.

Опыт Group-IB показывает, что Red Teaming и тестирование на проникновение отлично дополняют друг друга. Каждое исследование по-своему важно и полезно для организации, поскольку в ходе такой комбинированной атаки удаётся оценить как пассивную защиту систем, так и активную защищённость компании в целом.

Red Teaming дополняет другие формы тестирования (например, анализ кода, тестирование на проникновение и т.д.) и по мере роста организации включается в план по проверке информационной безопасности.

Основные отличия Red Teaming от Penetration Testing

	Red Teaming	Penetration Testing
Фокус проекта	Фокус на «глубину» исследования. Чем глубже прорабатывается цель, тем лучше Главная задача – проверить и усилить способность организации к обнаружению и реагированию на сложные кибератаки.	Фокус на «широту» исследования. Чем больше охват, тем лучше. Требуется охват наибольшего количества векторов атаки. Главная задача — взлом максимального количества систем и выявление максимального числа уязвимостей в ограниченный промежуток времени.
Методы и векторы атак	Все утвержденные методы, включая разрушительные, если применение таковых одобрено Заказчиком. Направлено на достижение согласованной цели, демонстрацию возможности критического воздействия на организацию, а также проверку людей, процессов и технологий.	Технические методы атаки на согласованный перечень объектов, за исключением разрушительных. Социальная инженерия, если ее применение разрешено Заказчиком. Ограниченный охват, нацелено на техническую проверку конкретных активов организации.
Соответствие	Исследование имитирует тактики, методы и инструменты реальных злоумышленников.	Исследование проводится в соответствии с методологией, принятой в индустрии.
Обход систем обнаружения	Важно обойти системы обнаружения вторжений, т.к. при их использовании правила игры меняются.	Важно выявить технические уязвимости системы, а не уклониться от систем обнаружения вторжений.
Пост-эксплуатационная активность	Эксплуатация уязвимости для захвата необходимых данных и дальнейшего развития атаки.	Если доступ к данным получен, тестирование завершается.
Результаты	• Подробный отчет с описанием предпринятых действий, результатов и способов достижения целей. • Детальная информация обо всех скомпрометированных активах и оценка способности Заказчика вовремя обнаружить и правильно среагировать на кибератаку	• Подробный отчет с описанием всех обнаруженных уязвимостей и уровней их риска. • Детальная информация о проведенных проверках и результатах их прохождения.

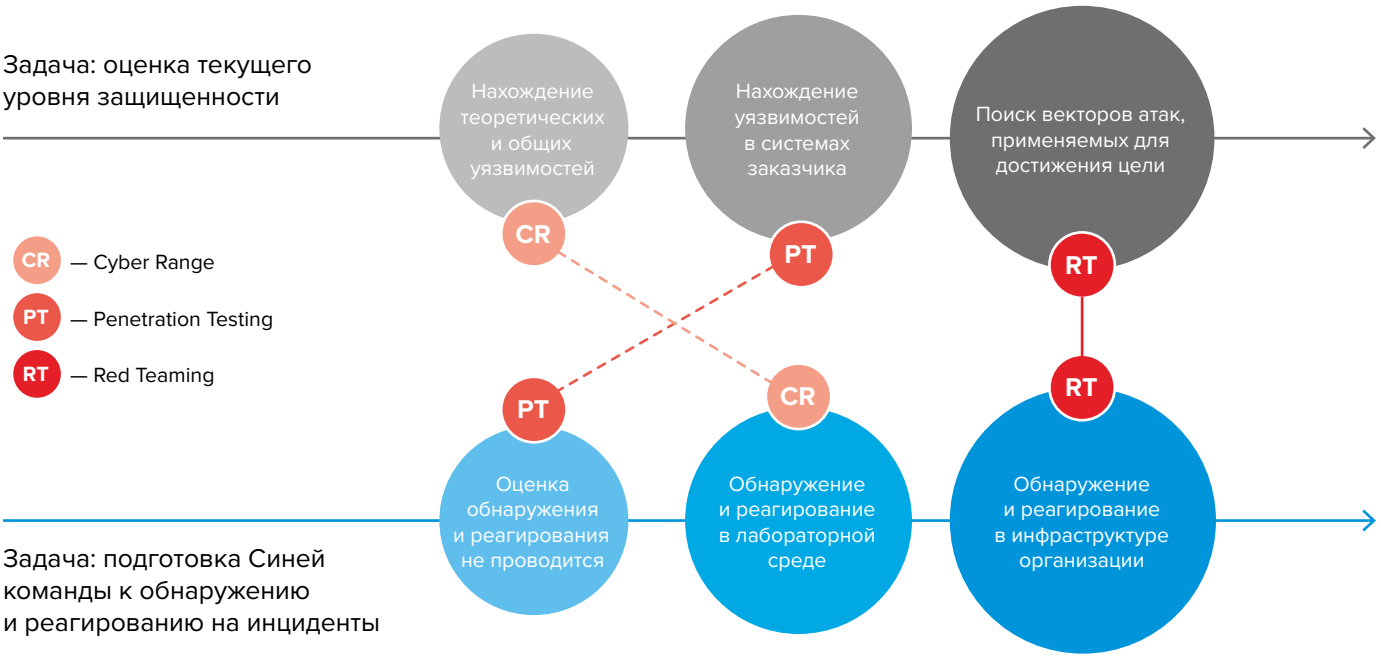


Рисунок 1. **Сравнение целей и результатов исследований, схожих с Red Teaming**

04

ПОДХОД GROUP-IB К RED TEAMING

Рисунок 3. **Распределение действий в рамках Red Teaming исследования**

Исследование в формате Red Teaming можно разделить на несколько последовательных стадий:

Рисунок 2. **Основные этапы Red Teaming исследования**

Для повышения эффективности некоторые действия внутри основных стадий могут начинаться раньше или выполняться параллельно с другими с учетом ограниченного времени. Поэтому на практике Red Teaming процесс не является такой четкой линейной последовательностью шагов.

Заинтересованные стороны (Заказчик и Исполнитель) должны придерживаться данных стадий работ в проведении Red Teaming, чтобы обеспечить стандартизацию процесса согласно всем требованиям.

Непосредственными сторонами, участвующими в процессе Red Teaming, являются:

от Заказчика:

- Белая команда — ответственный менеджер, представители бизнес-подразделений Заказчика и максимально необходимое количество экспертов по безопасности, которые будут знать о проведении работ.
- Синяя команда — служба безопасности Заказчика по обнаружению и реагированию на инциденты информационной безопасности.

Во время тестирования Белая команда взаимодействует с Красной командой и при необходимости вмешивается. Например, когда тестирование влияет на критически важные процессы.

от Исполнителя:

- Ответственный менеджер и Красная команда.

Ответственные менеджеры обеих команд тесно взаимодействуют друг с другом, чтобы правильно организовать процесс Red Teaming, договориться о сроках проведения работ и обеспечить прозрачность коммуникаций.

1. Подготовительная стадия

Продолжительность: 4-6 недель

Задача: оценить текущие потребности конкретной организации и объем работ.

План мероприятий:

- Создается рабочая группа из представителей Заказчика и Исполнителя;
- Определяется область работ (продолжительность, объем, юридические границы и запрещенные действия);
- Согласуются протоколы и форматы взаимодействия;
- Формируется Красная команда под потребности текущего проекта.

На этой стадии объявляется официальный запуск проекта.

Результаты:

- согласованная область тестирования;
- согласованные цели и задачи работ;
- утвержденный план проекта и способы коммуникации;
- сформированные рабочие группы для контроля мероприятий и управления ими.

2. Стадия проведения Red Teaming

Продолжительность: от 12 недель и более

На данной стадии Красная команда:

- Производит разведку в формате Threat Intelligence.
- Разрабатывает сценарии, основанные на критичных функциях систем и модели угроз.
- Формирует план и предпринимает попытки атак на согласованные цели (системы и службы, которые содержат одну или несколько критичных функций).

Стадия подразделяется на два основных этапа — разведка и разработка сценариев, а также само тестирование в формате Red Teaming.

Результаты:

- план тестирования;
- перечень сценариев потенциальных атак для дальнейшей проверки;
- технический отчет с результатами тестирования.

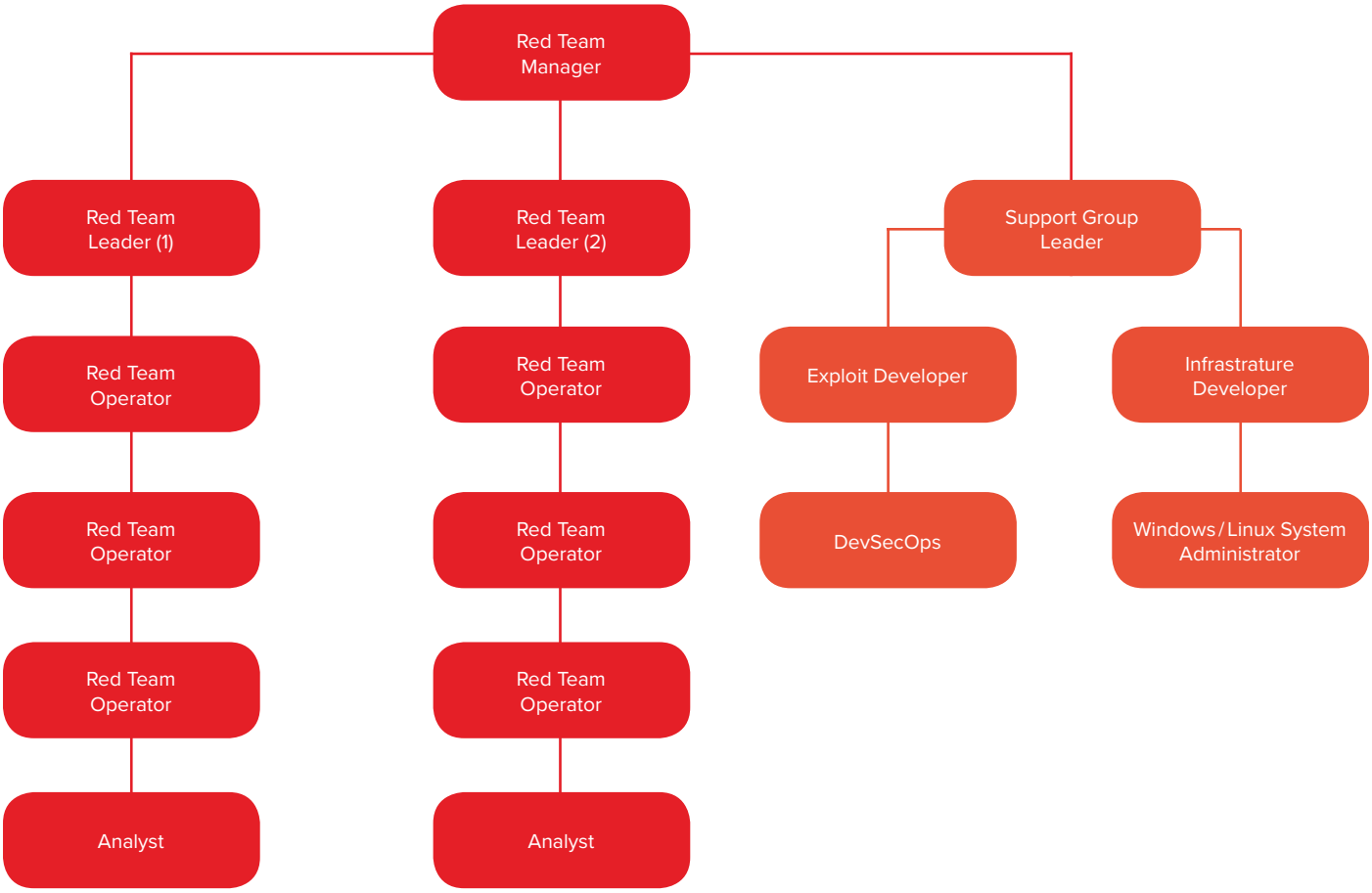


Рисунок 4. **Команда Red Teaming проекта**

Этап №1. Кибербразведка и сценарии

На данном этапе Красная команда проводит кибербразведку. Также Заказчик может обратиться к стороннему поставщику Threat Intelligence (TI) за целевым анализом угроз (TTI Report) для исследуемого объекта, который дополнит сценарии дальнейшего тестирования и предоставит полезную информацию о Заказчике.

Красная команда выполняет максимально обширную разведку, которую обычно производит злоумышленник при планировании целенаправленной атаки на организацию. Цель подобной разведки — изучить профиль, структуру и направление деятельности организации. Также она позволяет определить наиболее подходящие для организации угрозы и определить ключевые узлы и цели с точки зрения злоумышленника.

На основании проведенных работ составляются план тестирования и перечень практических сценариев потенциальных атак для дальнейшей проверки. Разработанные сценарии учитывают не только применяемые ранее подходы, но и новые методы соответствующих субъектов угрозы.

Этап №2 — Red Team тестирование

Действуя на основании плана и сценариев, сформулированных ранее, Красная команда:

- Выполняет скрытые атаки на идентифицированные критичные функции / активы целевых систем.
- Фиксирует ключевые точки — цели тестирования, которые согласовывались на предыдущем этапе и могли быть обновлены в процессе анализа целевых угроз.
- При возникновении препятствий Красная команда разрабатывает альтернативные способы достижения целей, используя тактики продвинутых злоумышленников.

Красная команда является динамической, т.е. может быть дополнена специалистами релевантного задаче профиля.

Все работы проводятся в тесном контакте с Белой командой, а все действия Красной команды записываются для подготовки отчета.

3. Заключительная стадия

Продолжительность: от 2 до 4 недель.

Тестирование Red Teaming официально завершается после того, как все шаги были успешно выполнены либо истекло выделенное на работы время.

На данной стадии:

- Оценивается способность Синей команды к обнаружению и реагированию на киберугрозы, которые производит Красная команда.
- Красная команда готовит отчет с описанием работ, выводами и наблюдениями и передает его Синей команде. При необходимости отчет дополняют рекомендациями по улучшению технического контроля, политик и процедур, а также повышению осведомленности сотрудников.
- Синяя команда получает информацию о проведенном тесте и на основании отчета Красной команды готовит собственный отчет, где отражает свои действия.
- Участники процесса обмениваются результатами, анализируют их и планируют дальнейшие шаги по повышению киберустойчивости организации.

Результаты:

- отчет Красной команды по проведенному тестированию и рекомендации;
- отчет Синей команды по проведенному тестированию и сверке результатов;
- мероприятие по совместному воспроизведению атак и противодействию им;
- план действий по стратегическому управлению безопасностью и общие выводы.

05 МЕТОДИКА ВЫПОЛНЕНИЯ РАБОТ

Для имитации атак на установленную цель специалисты Group-IB пользуются проверенной методологией, которая адаптируется под каждого конкретного Заказчика. Group-IB учитывает специфические требования и особенности деятельности организации, чтобы не нарушать непрерывность критичных бизнес-процессов.

Жизненный цикл тестирования в формате Red Teaming проходит по модели The Cyber Kill Chain и имеет следующие обобщенные шаги: разведка, вооружение, доставка, эксплуатация, инсталляция, получение управления и выполнение действий в отношении цели. Продвинутые кибератаки, которые проводит Красная команда, включают целую серию шагов, предпринимаемых для выполнения миссии.

Разведка

Сбор как можно большего количества информации о цели.

Это один из самых важных шагов, который позволяет узнать много нового о людях, технологиях и окружении. Этап может включать приобретение специальных инструментов и данных.

Вооружение

Анализ собранной информации об инфраструктуре, объектах и сотрудниках.

Посредством тщательного анализа Красная команда начинает формировать план достижения цели и основные операции для его достижения.

Доставка

Активный запуск полной Red Teaming операции. Красная команда проводит социоинженерные атаки, анализ уязвимостей, установку различного программного обеспечения для поддержания удаленного соединения, а также определяет наилучшие условия для дальнейшей эксплуатации.

Эксплуатация и инсталляция

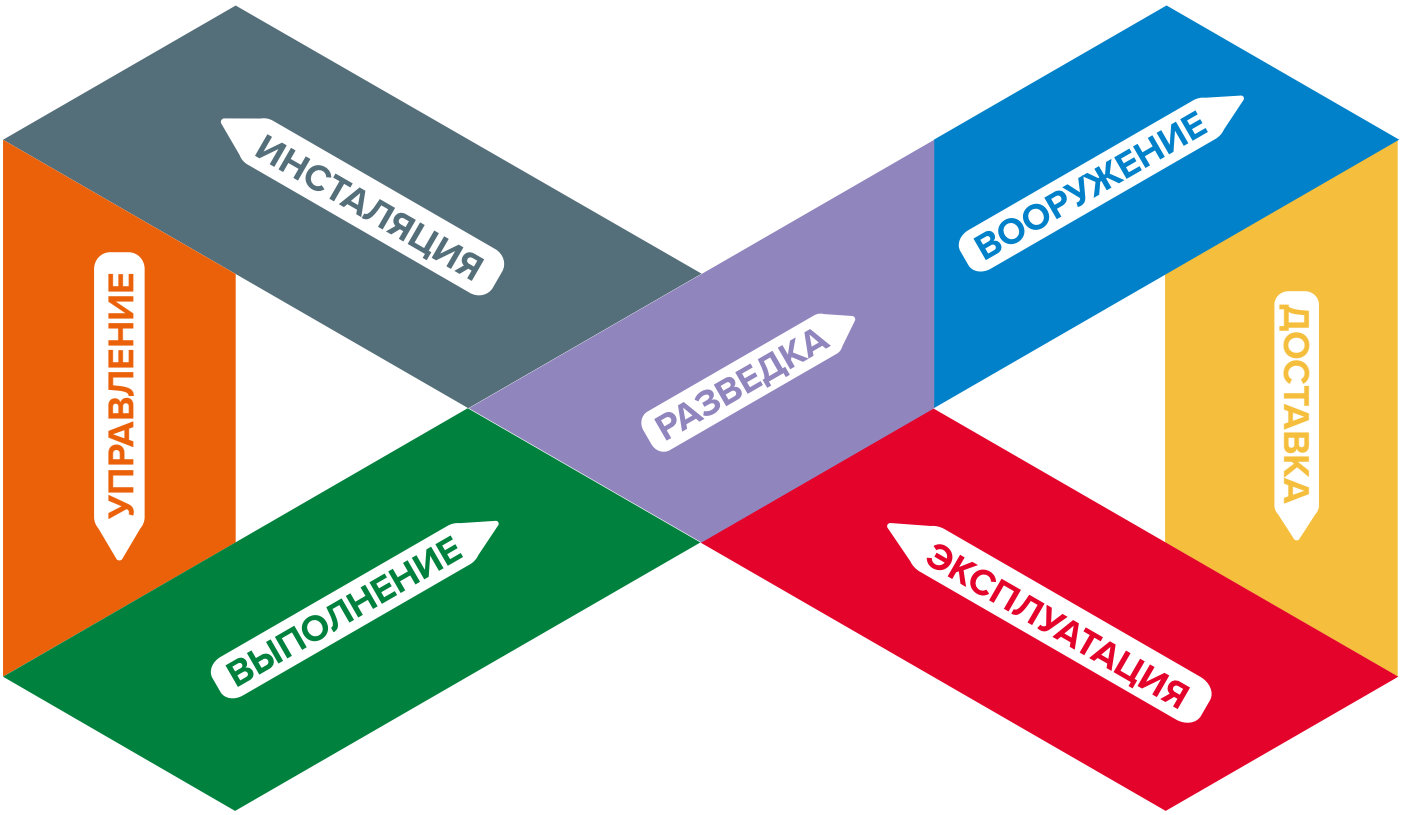
Основная задача на данной стадии — проложить путь к следующему этапу получения управления. Красная команда «взламывает» серверы/приложения/сети и эксплуатирует целевой персонал с помощью социальной инженерии.

Получение управления

После успешной компрометации предпринимаются попытки перейти от изначально от изначально скомпрометированных систем к более уязвимым или высокоценным. Например, «переключение» между внутренними системами, непрерывное повторное использование любого расширения доступа для того, чтобы в итоге поставить под угрозу согласованные целевые системы.

Выполнение действий

Задача Красной команды на данном этапе — открыть доступ к скомпрометированным системам и к ранее согласованным целевым данным. Красная команда стремится максимально эффективно завершить работы и достичь согласованных ранее целей.



Подготовка
- Определение цели, подбор инструментов
- Сбор данных об инфраструктуре и сотрудниках, тестирование на обнаружение

Получение доступа
- Подготовка к эксплуатации
- Получение первоначального доступа
- Закрепление в системе

Эксфильтрация данных
- Организация канала управления
- Расширение привилегий, кража данных и сокрытие следов

Рисунок 5. **Методика Red Team исследования**

06 КЕЙСЫ RED TEAMING ОТ GROUP-IB

КЕЙС 1

Получение доступа к Active Directory

Заказчик: группа компаний (производство).

Цель: получение административного доступа к контроллеру домена Active Directory в штаб-квартире компании.

Ситуация: заказчик использует многофакторную аутентификацию (смарт-карты) для всех типов доступа в штаб-квартире, включая удаленные и внешние веб-службы (см. Рисунок 6). Применение социальной инженерии запрещено.

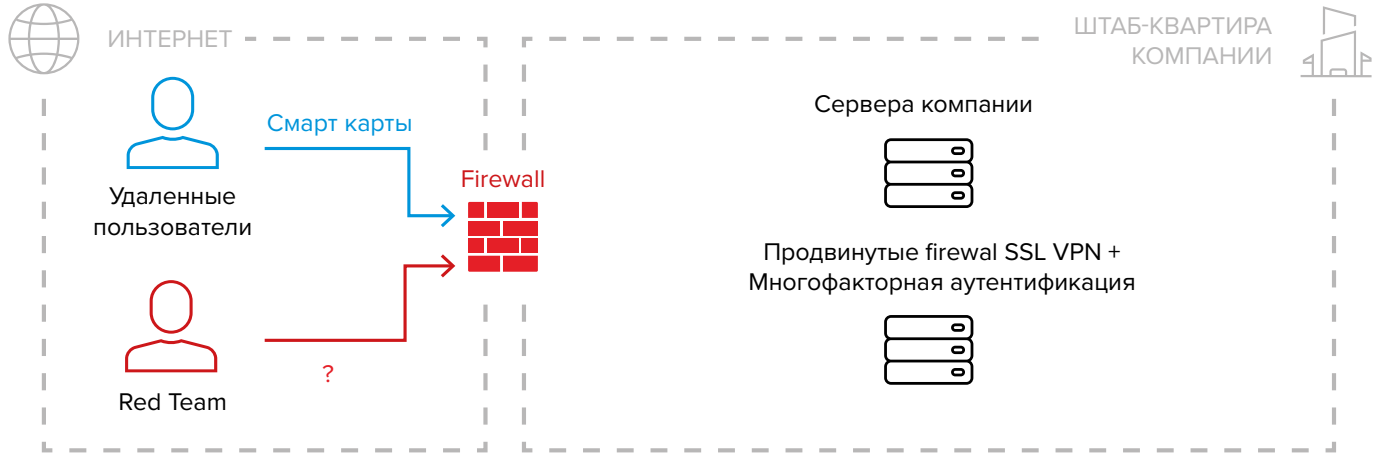


Рисунок 6. **Инфраструктура промышленной компании**

Действия Group-IB и результаты

Была проведена тщательная разведка. Установлено, что штаб-квартира приобрела 14 компаний и проводила их реорганизацию в свои филиалы во время проведения операций Red Team. Команде Group-IB Red Team удалось получить разрешение на проведение атаки на все компании группы. Далее была взломана дочерняя компания со слабой защитой, в том числе контроллеры домена branch1.domain.com, и обнаружен VPN между локальными сетями подразделений (site-to-site full-mesh VPN).

У Заказчика был наполовину построен лес доменов Active Directory для всех филиалов, но он не смог хорошо укрепить внешнюю сеть (рисунок 7).

Подключение к сети было хорошо защищено. Механизмы доверия между доменами леса Active Directory не работали для контроллеров на домене branch1.domain.com. Атаку удалось распространить на branch2.domain.com, получив там права администратора домена.

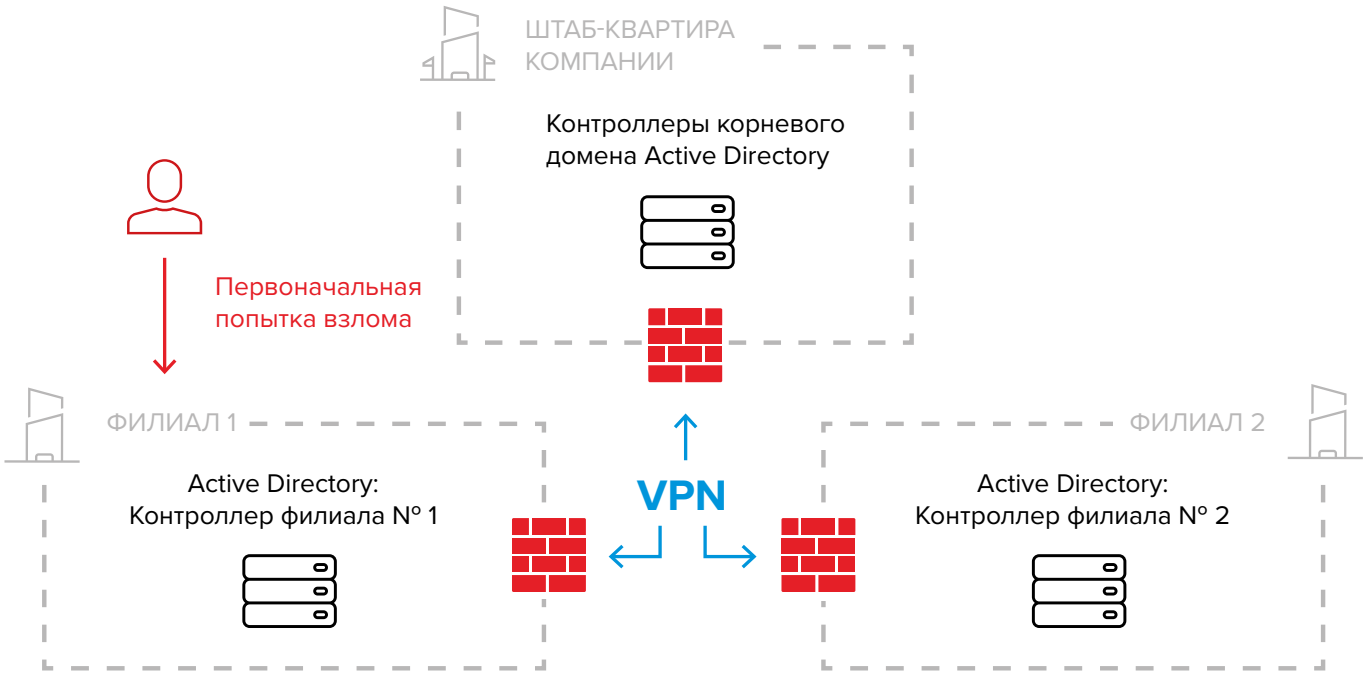


Рисунок 7. **Первоначальная попытка взлома Active Directory**

Применяя атаку Kerberos **"**golden ticket**"**, Red Team обошла защиту с помощью смарт-карт на низком уровне за счет особенностей реализации самого протокола Kerberos. Эксплуатируя механизм доверия между доменами Active Directory, удалось получить администраторские права в головном офисе (рисунок 8).

Контроллеры домена в штаб-квартире были взломаны: специалисты Group-IB достигли цель Red Teaming проекта.

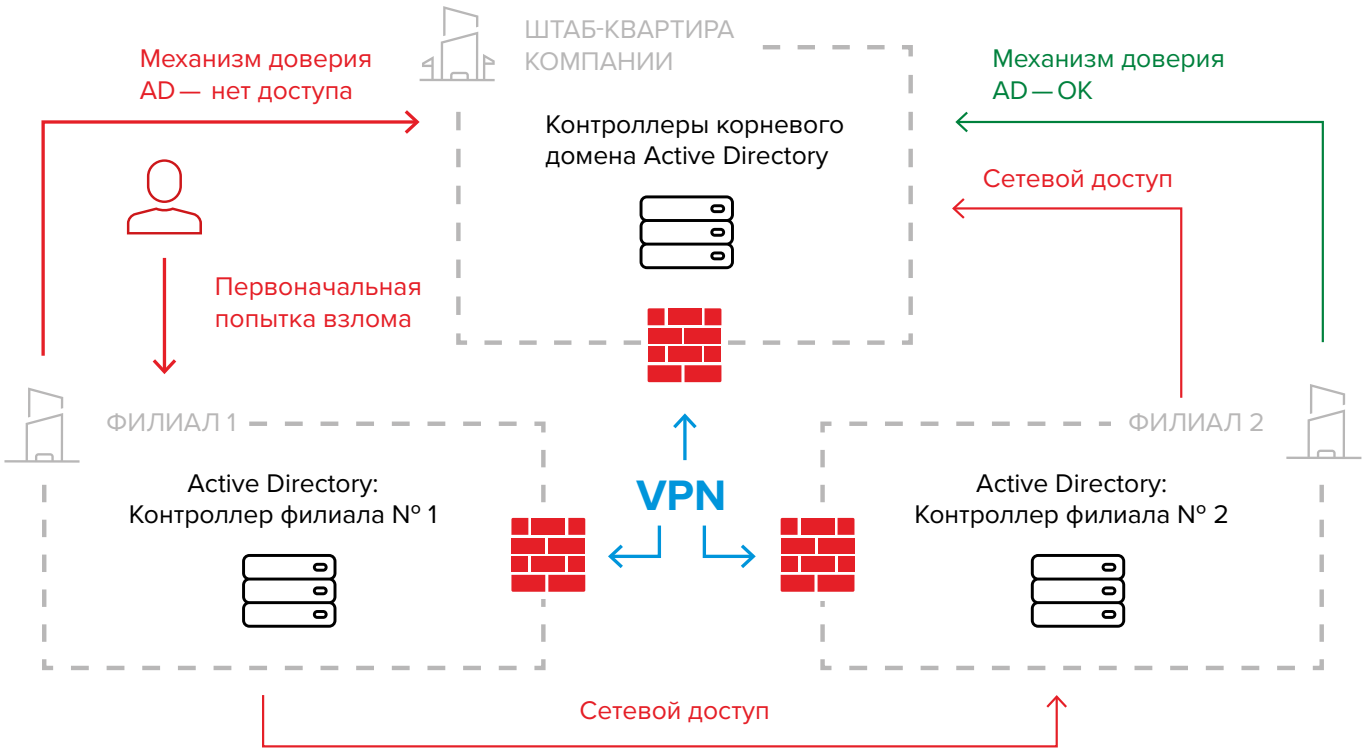


Рисунок 8. **Получение доступа к Active Directory**

КЕЙС 2

Получение доступа к финансовым системам

Заказчик: крупная розничная компания.

Цель: получение доступа к внутренним финансовым системам в штаб-квартире.

Ситуация: внешний сетевой периметр штаб-квартиры включал несколько доступных извне серверов, которые были хорошо защищены. Большинство систем — облачные и общедоступные. Применение социальной инженерии запрещено. Атаки на филиалы организации не были разрешены, так как клиент считал это неэффективным вектором атак: филиалы не были подключены к информационным системам головного офиса (рисунок 9).

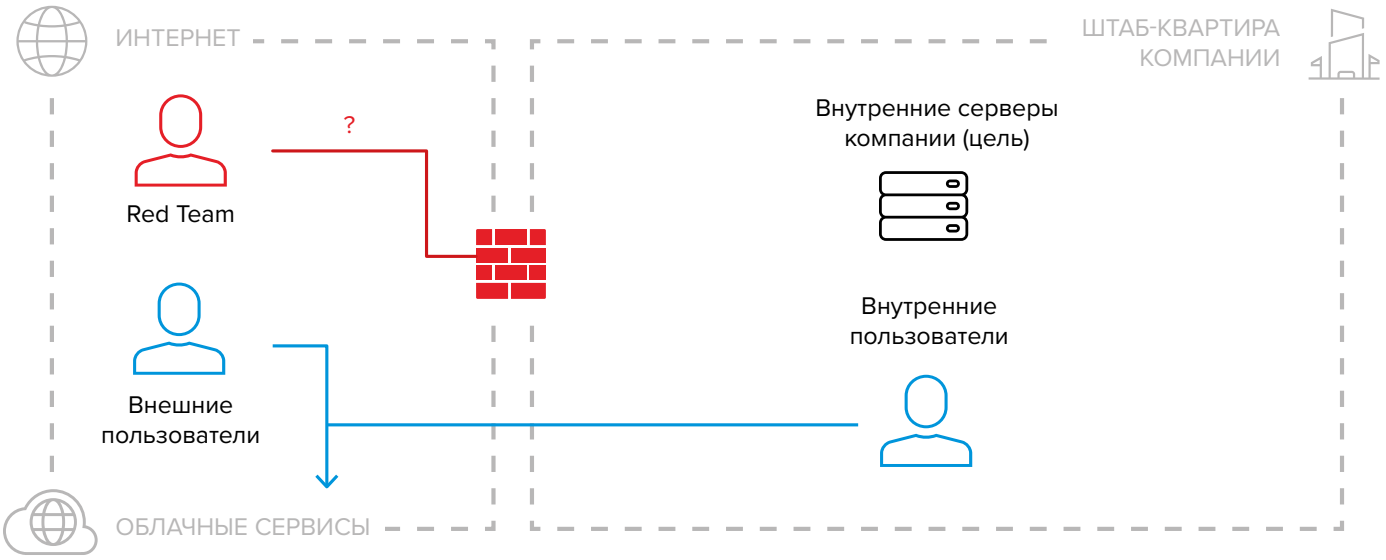


Рисунок 9. **Инфраструктура розничной компании**

Действия Group-IB и результаты

Команда Group-IB Red Team установила, что сервер одной из компаний-подрядчиков Заказчика был указан в публичной почтовой записи DNS SPF и мог отправлять электронные письма от имени компании. Этот сервер не входил ни в один общедоступный облачный сервис, и потребность в нем была неизвестна. Сервер имел несколько веб-страниц, которые находились в стадии разработки и были связаны с Заказчиком, а также порт OpenVPN TCP с нестандартным номером — такой же, как и у одного из серверов Заказчика на его внешнем сетевом периметре. Это могло косвенно свидетельствовать о наличии туннеля между сервером и локальной сетью Заказчика. Red Team выявила владельца сервера, связалась с ним и смогла получить официальное разрешение на проведение тестирования на проникновение в обмен на бесплатный мини-отчет о фактической защищенности данного сервера (рисунок 10).

Команда Group-IB Red Team взломала сервер и обнаружила, что на нем находится несколько систем в стадии разработки, созданных субподрядчиком для Заказчика. Сервер по сути выступал тестовой площадкой для этих сервисов. Более того, для выгрузки данных из внутренних систем организации на этот сервер Заказчик ранее создал VPN-туннель до своей локальной сети. Изначальное предположение команды Red Team подтвердилось. Red Team скопировала OpenVPN конфигурацию и получила доступ к сети. VPN был неправильно

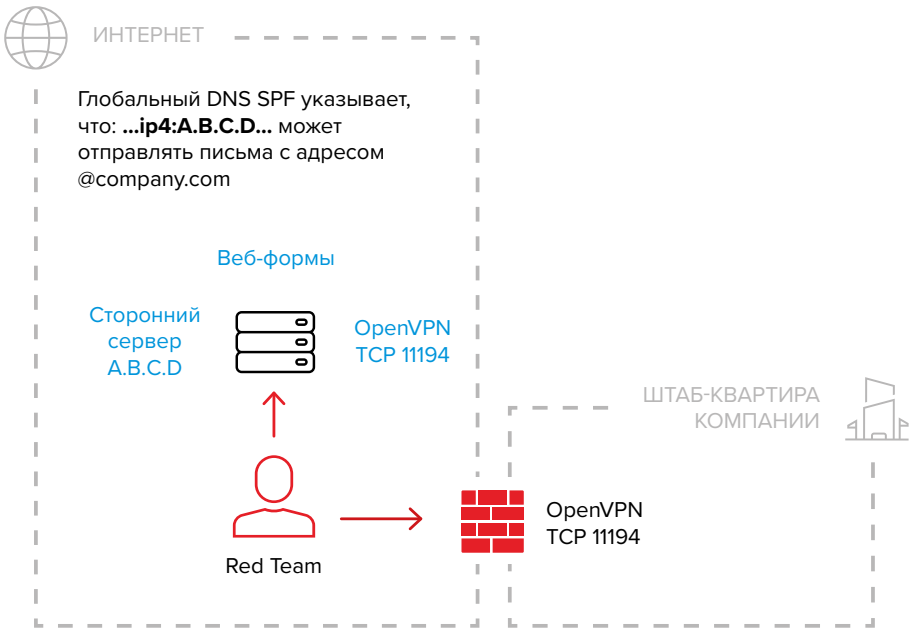


Рисунок 10. **Сервер компании-подрядчика с портом OpenVPN TCP**

сконфигурирован: список доступных IP-адресов внутри сети сети Заказчика был ограничен только маршрутизацией на клиенте OpenVPN (рисунок 11).

Если переконфигурировать маршруты на клиенте, VPN получал неограниченный доступ в локальную сеть. После получения первоначального доступа к локальной сети Red Team использовала типичные методы атаки на сети на основе Windows (lateral movement) для получения прав администратора домена Active Directory и доступа к внутренним финансовым системам.

Таким образом, специалисты Group-IB достигли цель Red Teaming проекта.

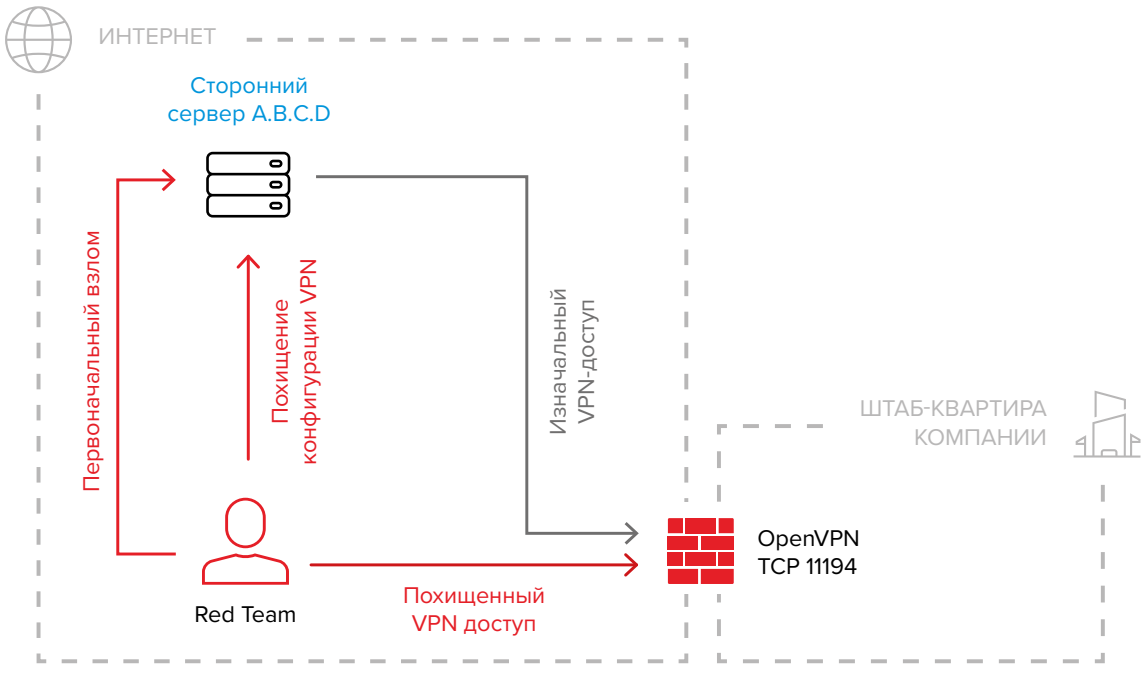


Рисунок 11. **Получение неограниченного доступа в локальную сеть**

07 ЗАКЛЮЧЕНИЕ

Тестирование в формате Red Teaming дает организации представление о мере готовности организации к выявлению и отражению сложных кибератак, а также позволяет оценить и определить план будущих улучшений в этой области.

Исправление недостатков, обнаруженных в ходе Red Teaming, позволит обеспечить непрерывность бизнес-процессов и защиту ценных данных.

Ключевые возможности Red Teaming:

- оценить киберриски для самых важных активов;
- обнаружить неизвестные уязвимости и слабые стороны;
- проверить правильность работы всех систем и процессов безопасности;
- определить сильные и слабые стороны внутренней команды безопасности;
- повысить способность реагирования на кибератаки;
- усовершенствовать подход к обеспечению кибербезопасности.

Проводя Red Teaming и практикуя реагирование на контролируемые атаки, внутренняя команда безопасности может улучшить свои способности по обнаружению ранее незамеченных угроз, чтобы остановить реальных злоумышленников на ранних стадиях атаки и предотвратить материальный и репутационный ущерб для бизнеса.

Таким образом, добавив Red Teaming в часть стратегии по безопасности, компания может измерять улучшения в безопасности с течением времени. Подобные измеримые результаты можно использовать для экономического обоснования дополнительных проектов по информационной безопасности и внедрения необходимых технических средств защиты.

GROUP-IB

Group-IB — одна из ведущих международных компаний по детектированию и предотвращению кибератак, выявлению фрода и защиты интеллектуальной собственности в сети.

По версии **Gartner, IDC и Forrester,** Group-IB является одним из ключевых поставщиков Threat Intelligence в мире, в базе которой хранится 100 000+ профайлов киберпреступников.

Клиентами Group-IB являются крупнейшие банки и финансовые организации, промышленные и транспортные корпорации, ИТ и телеком провайдеры, ритейл и FMCG компании в 60 странах мира.

55 000+
часов реагирования

1000+
успешных расследований по всему миру

OSCE — Рекомендована Организацией по Безопасности и Сотрудничеству в Европе (ОБСЕ)

EUROPOL INTERPOL — Официальный партнер

FIRST TI — CERT-GIB - центр круглосуточного реагирования на инциденты информационной безопасности – аккредитованный член международных сообществ FIRST и Trusted Introducer.

Узнать больше о Group-IB Red Teaming

group-ib.ru/red-teaming
ac@group-ib.com