почему матерые пентестеры лажают в Red Team / Хабр

habr.com/ru/companies/bastion/articles/829402

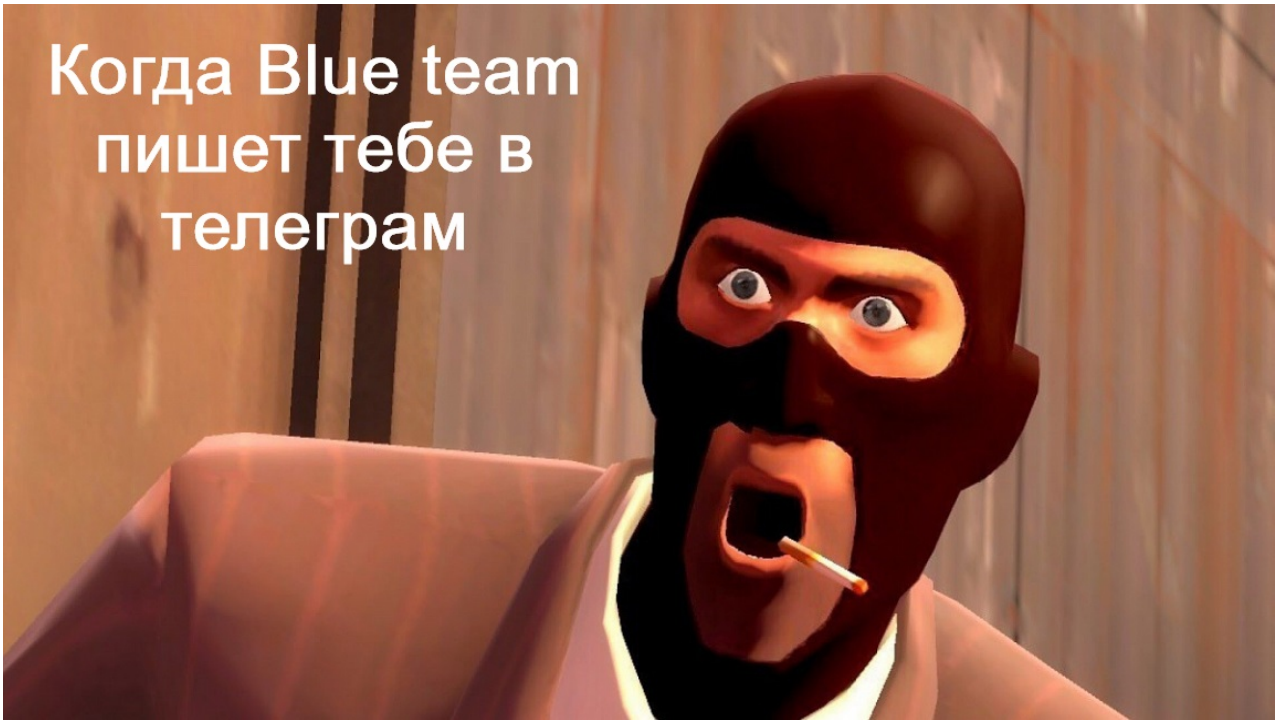
secm3n

secm3n 17 июл в 16:22

Красная команда, черный день: почему матерые пентестеры лажают в Red Team

12 мин

8.4K
Кейс



Как правило, заказы на Red Team поступают к уже опытным хакерским командам, которые набили руку на многочисленных пентестах. У них есть проверенные тактики и методы взлома, а также уверенность в своих силах. А ещё иногда они совершают «детские» ошибки во время первых редтимингов в карьере. Знаю это по собственному опыту.

В этой статье тряхну стариной и расскажу об одном из первых Red Team-проектов:

1. Разберу различия между Red Team и пентестом с точки зрения исполнителя.

2. Поделюсь приемами оффлайн-разведки и рассмотрю процесс поиска уязвимостей на примере реального кейса.
3. Покажу типичные ошибки, которые совершают пентестеры, переходящие в Red Team.

Даже опытные специалисты не всегда видят тонкие различия между пентестами и Red Team. Разница кроется в подходе к выявлению уязвимостей и оценке безопасности организации.

Задача **Red Team** — смоделировать реальную кибератаку. Команда ищет критические уязвимости для достижения конкретной цели или нескольких целей, например, похищения коммерческой тайны. Команда ИБ заказчика не в курсе того, что происходит и может активно препятствовать редтиму в случае обнаружения.

Пентест выполняется в совсем других условиях: у пентестеров есть цель, достигнуть которой команда пытается одним единственным способом, оговоренным ранее (если заказчик не просит иного). Более того, служба ИБ заказчика всегда в курсе действий пентестеров и никак не препятствует им.

Ключевая особенность Red Team — скрытность действий. Команда минимизирует следы и старается не привлекать внимание службы безопасности компании. Это позволяет оценить компетенцию ИБ-специалистов заказчика. Red Team максимально приближен к реальным атакам, тогда как пентест — более формализованное мероприятие. Он часто включает общение обмен информацией с ИБ-службой и администраторами заказчика.

	Red Team	**Пентест**
Методы и цели	Подразумевает комбинацию различных подходов: социальная инженерия, имитация реальных атак, OWASP Testing Guide, MITRE ATT&CK Framework, SANS Penetration Testing Framework, Information Systems Security Assessment Framework (ISSAF), PTES. Цель — проверить скорость и качество реакции Blue Team.	Структурированная методология, нацеленная на поиск и эксплуатацию технических уязвимостей в сетях и системах. Цель — выявить угрозы и предоставить рекомендации по их исправлению.

	Red Team	Пентест
Подход	Команда работает в реальной среде, средства защиты не отключены. Возможно активное противодействие со стороны клиента. Если действия Red Team разоблачают, проект считается завершенным.	Служба ИБ заказчика знает о времени начала и окончания тестирования, а также об основных этапах и условиях проведения пентеста. Между службой ИБ и пентестерами идет обмен информацией. Заказчик не только не мешает, а порой даже помогает в отдельных аспектах работы.

Оба подхода — Red Team и пентест — позволяют оценить уровень защищенности компании, но проводятся в разных условиях. Чтобы наглядно это показать, я обратился к старым записям. Расскажу, как команда, с которой я работал, проводила свой первый Red Team.

Редтиминг на практике. Постановка задачи

Нам предстояло исследовать компанию, оказывающую финансовые и кредитные услуги гражданам. Назовем ее Компания-Которую-Нельзя-Называть (ККНН). Некоторые детали и часть наших действий я скрою в интересах заказчика. Суть сохранится, но рассказ станет чуть проще и короче.

Мы должны были провести тестирование на проникновение методом Red Team, имитируя действия злоумышленников. О предстоящей атаке знал только директор службы информационной безопасности компании. В качестве целей заказчик выбрал разные компоненты корпоративной инфраструктуры:

- Хранилище аналитических данных (DWH);
- Базы с персональными данными клиентов и некоторые компоненты 1С;
- Бэкапы.

В идеальном исходе событий мы должны были справиться с задачей так, чтобы ИБ-служба ничего не заметила. А как оно было в реальности?

Активный и пассивный сбор информации

В начале проекта пентестеры обычно находятся в более выгодном положении: заказчик предоставляет им всю необходимую информацию: список доменов компании или диапазон IP-адресов для проверки. Исполнители часто согласуют свои действия с ИБ-службой, например при использовании эксплоитов в рабочей инфраструктуре, и не тратят время на бесперспективные векторы атак.

Red Team работает иначе: у нас было только название компании, а всю информацию об IT-инфраструктуре заказчика пришлось искать самим. Нас интересовали данные об офисах, сотрудниках, подрядчиках, клиентах и партнерах заказчика: эти люди могли иметь доступ к инфраструктуре или корпоративным сервисам.

Для пассивной разведки мы использовали несколько десятков утилит, включая HackerTarget, Hunter, IntelX, IPdata, IPinfo и NetworksDB, работающих с протоколами DNS, BGP и SSL-сертификатами. В результате мы обнаружили:

- Несколько дочерних проектов помимо основного сайта компании. Также выделили CIDR, относящийся к инфраструктуре заказчика.
- Местоположение офисов и документацию из открытых источников о физической защите объектов.
- Несколько тысяч корпоративных адресов электронной почты сотрудников, некоторые адреса фигурировали в парольных утечках.

Увы, мы не смогли использовать выявленные учетные данные для доступа к корпоративным сервисам — пароли уже сменили. Атаки Password Spraying с утёкшими email-адресами и распространёнными паролями тоже не удались.

Мы попытались провести фишинговую рассылку по адресам руководителей, чтобы получить первоначальный доступ в сеть заказчика, но и тут столкнулись со сложностями. Позже мы изучили почтовые ящики сотрудников и выяснили, что письма были распознаны СЗИ как фишинговые: поэтому они попадали в карантин.

Затем мы перешли к активной разведке. С помощью инструментов DNS-разведки мы составили список поддоменов в доменных зонах компании и просканировали работающие там сервисы.

Хотя легких путей мы не обнаружили, нам удалось собрать информацию для дальнейшей работы. Приоритетными целями для тестирования стали:

1. Основной веб-сайт и его API.
2. Сервисы, функционирующие в домене.
3. Офисы компании, которые мы решили посетить лично и разместить там закладки.

Тестирование внешнего сетевого периметра

Мы проанализировали сайт ККНН и нашли несколько критических уязвимостей. Их эксплуатация могла привести к массовой утечке конфиденциальной информации и персональных данных. Одна из них — классический IDOR (Insecure Direct Object References).

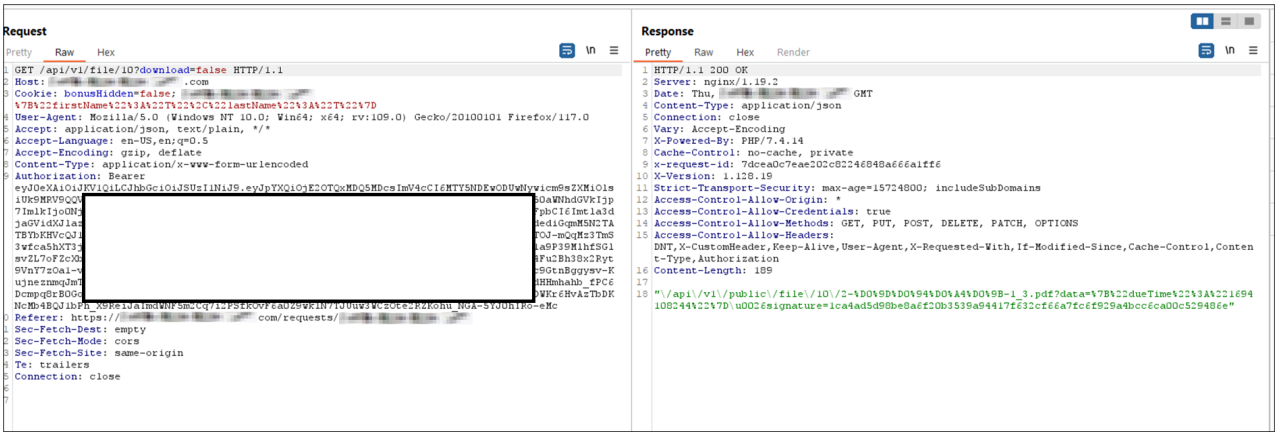
Доступ к некоторым объектам в системе был реализован по прямой ссылке с уникальными идентификаторами. Однако система не проверяла, принадлежит ли запрашиваемый идентификатор пользователю. К тому же сами идентификаторы имели слабую энтропию, что делало их уязвимыми к перебору.

```
GET /api/v1/file/1337/preview/big HTTP/1.1
Host: KHHH.com
Cookie: bonusHidden=false;
_platform=%7B%22firstName%22%3A%22T%22%2C%22lastName%22%3A%22T%22%7D
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/117.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Authorization: Bearer [..]
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Отправив GET-запрос вида */api/v1/file/1337/preview/big* с произвольным числовым идентификатором файла, можно было получить доступ к базе с паспортами, договорами и другими документами клиентов ККНН. Это была большая база: свежезагруженные файлы получали идентификатор с номером более чем 3 000 000.

Демонстрация наличия IDOR

То же самое происходило при обращении методом GET к API: /api/v1/file/10?download=false.



Мы также обнаружили возможность внедрения произвольного кода в SQL-запрос в форме поиска личного кабинета на сайте. Эту уязвимость можно было реализовать с использованием Boolean-based техники. При таком сценарии атакующий получает разное содержимое в зависимости от логического результата (True или False) при отправке запроса к базе данных.

Саму уязвимость можно продемонстрировать двумя запросами. Если сравнить длину ответов, станет ясно, что они отличаются. Это происходит из-за того, что в первом случае в SQL-запрос внедрено условие, которое возвращает значение True, а во втором — False. Для упрощения работы с этим типом атак часто используется инструмент под названием sqli_blinder.

В итоге нам удалось извлечь из базы refresh-токены административной учетной записи.

Компрометация refresh-токенов административной учетной записи

Помимо этих уязвимостей, мы выявили еще несколько десятков менее серьёзных багов. В результате мы получили доступ к некоторым базам с персональными данными, но не нашли ничего, что помогло бы проникнуть во внутренний контур компании.

Это ожидаемый результат. По нашей статистике, успешно пробить веб и развить атаку в корпоративной сети удается примерно в 10% случаев. Возможно, дело в том, что мы часто работаем с крупными компаниями, у которых достаточно зрелые ИБ-процессы и сервисы. Эти компании уже многократно пытались взломать до нас — и коллеги-пентестеры, и злоумышленники. Поэтому вопросам безопасности здесь уделяется много внимания, в том числе на уровне архитектуры. Например, внешние сервисы могут быть надежно изолированы от корпоративных сетей.

Физическое проникновение в офисы заказчика

Часто инфраструктуру крупных компаний проще взломать оффлайн. Поэтому параллельно с внешним пентестом мы отправили своих агентов в офисы заказчика.

Сначала они занялись OSINT: изучили YouTube-канал компании и посмотрели плейлисты с HR-материалами. По видео можно понять примерную планировку офисов, организацию прохода внутрь, расположение розеток и даже слепые зоны камер видеонаблюдения и использовать эту информацию в своих целях.

Первый объект

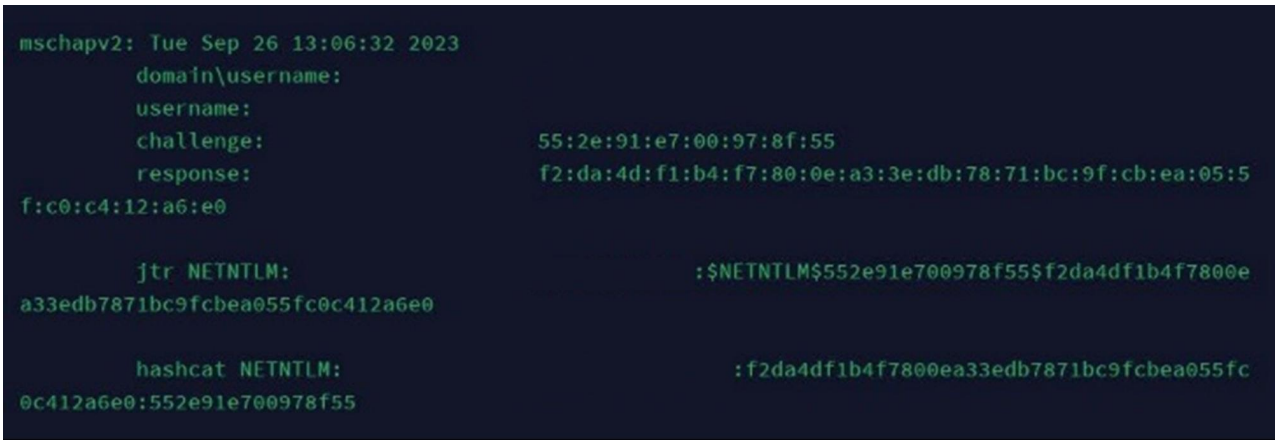
В первом офисе нам повезло: там проходил открытый для всех желающих митап по информационной безопасности в финансовой сфере. Мы совместили приятное с полезным — послушали доклады и нашли в холлах удобные RJ-45 розетки. Однако

мы решили не устанавливать проводные закладки, так как не смогли точно определить, какие розетки относятся к ЛВС заказчика, а какие — к сетям соседей-арендаторов.

Оставался другой вариант — поработать с корпоративной Wi-Fi сетью. Для аудита использовали wifite. WPA-E с проверкой подлинности клиентов делал сеть устойчивой к типичным атакам на протоколы WPA/WPA2/WPS. Поэтому мы решили вернуться в офис на следующий день и установить там поддельную точку доступа.

Попасть внутрь после окончания митапа не получилось. Нам повезло — у сети был хороший сигнал и за пределами охраняемой территории например, в столовой бизнес-центра, куда можно было попасть с помощью временного пропуска. Именно там мы применили технику EvilTwin в связке с GTC Downgrade.

Дело в том, что клиенты и серверы аутентификации обычно настроены на поддержку различных методов EAP: это помогает снизить вероятность проблем с несовместимостью устройств. Среди этих методов есть и небезопасные — EAP-GTC и EAP-PAP. Атака GTC Downgrade — это атака на понижение версии EAP. С ее помощью можно заставить жертву пройти аутентификацию на поддельной точке доступа с использованием слабо защищенного метода EAP, который подразумевает передачу учетных данных в виде открытого текста или NetNTLM-хэшей.



В тот день при помощи eaphammer мы скомпрометировали 27 учетных записей: 22 пароля были получены в чистом виде, 5 — в виде хеша NetNTLM. Валидация перехваченных пар «логин-пароль» прошла успешно, мы получили доступ в домен и собрали информацию об объектах Active Directory с помощью BloodHound для дальнейшего анализа.

Учетные записи, полученные в ходе этой атаки, пригодились на следующих этапах редтиминга. Кроме того, мы спрятали в здании сетевой имплант — Android-смартфон с доступом в интернет, разблокированным загрузчиком и установленным Nethunter. Однако сигнал был нестабильным, поэтому продуктивно работать на постоянной основе через этот канал связи не получалось.

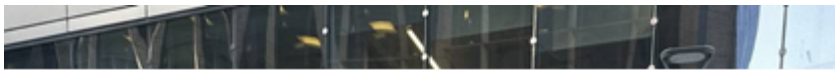
Второй объект

Работа со вторым офисом ККНН сначала не задалась. Попасть внутрь не получилось даже при помощи лестницы и рабочего комбинезона. Кроме шуток, образ электрика служит универсальным пропуском почти в любой бизнес-центр, но

здесь трюк не сработал. Пришлось снова искать места, где можно поймать корпоративный Wi-Fi:

- Платная парковка в непосредственной близости от здания.
- Курилка для сотрудников и клиентов возле главного входа.
- Расположенный неподалеку ресторан.

Основная проблема заключалась в том, что нам негде было «закрепиться» для спокойной работы: нужно было оккупировать строго определенный столик в ресторане, либо часами дымить в курилке. В итоге мы на неделю арендовали каршеринговый автомобиль, который пригнали ночью на парковку и оставили в зоне покрытия целевой сети.



В багажнике спрятали набор из усиленной Wi-Fi антенны (Alfa AWUS036NHA), ноутбука и 4G-модема. Запитали все это от пары автомобильных аккумуляторов и подключались через AnyDesk. Наконец у нас появился стабильный удаленный канал связи с внутренней сетью заказчика.

Исследование корпоративной инфраструктуры

Наладив связь, мы использовали учетные данные, полученные в первом офисе. Нам удалось войти в электронную почту сотрудников и сервисы Office 365 (SharePoint, Teams). Успех был обусловлен отсутствием двухфакторной аутентификации, которую администраторы компании не настроили.

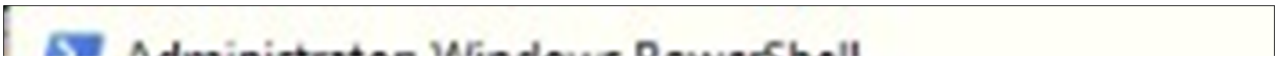
В почтовых ящиках мы нашли учетные данные для других сервисов, а также инструкции и настройки корпоративной VPN-сети. Подключиться к VPN без второго фактора не получилось, но вход в 1C и data-docs прошел беспрепятственно.

Наиболее ценная находка ждала нас на одном из файловых серверов — файл экспорта 1Password, который содержал 163 уникальные записи с учетными данными от различных систем.

Получение файла с паролями

Локальные учетные записи

В файле 1Password мы нашли пароль от локальной учетной записи sadmin. Эта запись имела права локального администратора на нескольких серверах BPA.

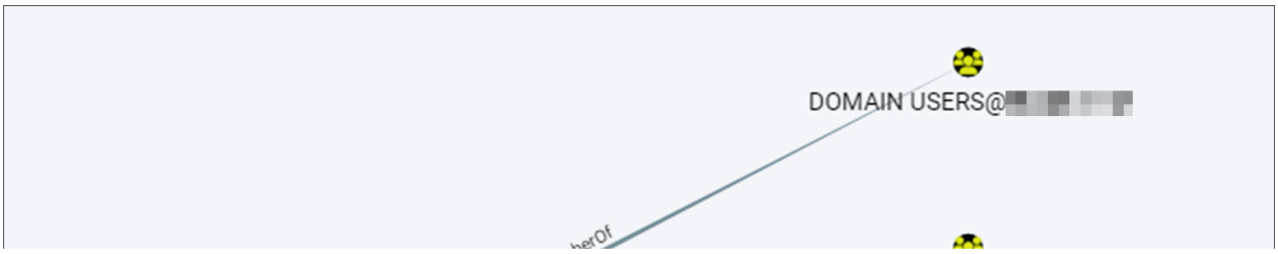


На серверах не был настроен сбор событий для последующего анализа логов. Кроме того, они имели выход в интернет.

К хостам применялась групповая политика, отключающая аудит

Эти серверы могли стать отправной точкой для атаки на организацию. Однако в этот момент служба безопасности что-то заподозрила и заблокировала одну из тех учетных записей, которые мы использовали параллельно. В ответ мы решили использовать другой вектор атаки, который казался более перспективным.

Все в том же экспорте 1Password мы обнаружили учетную запись, входящую в группу «Account Operators». Эта группа является одной из самых опасных из-за привилегий GenericAll над пользователями, компьютерами и другими группами. Исключения составляют лишь встроенные группы, такие как Domain Admins, Administrators, Backup Operators.



Нам удалось обнаружить учетные данные сотрудника технической поддержки, который входил в эту группу. Мы обнаружили, что в поле атрибута Description прописан путь к общему ресурсу «\сервер\Shared_Folders\IT» и предположили, что этот каталог может содержать ценную информацию. Поэтому было решено попытаться получить доступ к файловой системе сервера, на котором находился этот ресурс.

Чтение атрибута ms-msc-admpwd

Группа Account Operators обладает правами GenericAll над объектами домена. Это позволяет ей читать атрибут ms-msc-admpwd (LAPS) и получать пароль локальной учетной записи. А имя локальной учетной записи мы нашли в групповой политике local server admin, в которой стандартное имя administrator было изменено на sadmin.

Следующим шагом стало получение доступа к файловой системе, но полезной информации там не нашлось.

Доступ на диск D$

Доступ к центру сертификации

Атака затягивалась. Мы несколько дней исследовали домен и начали беспокоиться о возможной потере доступа к учетной записи из группы Account Operators. Без нее мы потеряли бы шансы добраться до хранилища аналитических данных (DWH) и бекапов.

Чтобы закрепиться в инфраструктуре, мы решили получить корневой сертификат с центра сертификации. Это позволило бы выпускать поддельные сертификаты для любого пользователя.

Членство в группе servers_admins давало нашей учетной записи права локального администратора на сервере. Групповая политика rdp certificate требовала наличия сертификата на стороне клиента, иначе подключиться к серверу по RDP было невозможно. Поэтому мы использовали технику PSRemoting для удаленного доступа к нужному серверу, после чего создали резервную копию сертификата центра сертификации.

Мы также создали дамп LSA, содержащий информацию о локальных учетных записях.

Домен заказчика работал на версии 2012 года. Это ограничивало возможности PKINIT, например, мы не могли получить TGT билет Kerberos с помощью сертификата. Однако сертификат все еще можно было использовать для техники Pass-The-Cert.

Pass-The-Cert позволяет использовать сертификат для подключения к LDAP. С его помощью можно выполнять различные запросы, например, создавать пользователей и добавлять их в группы при наличии соответствующих прав.

Результат техники Pass-the-Cert

Таким образом, созданную нами копию сертификата потенциально можно было использовать для генерации сертификата для любого пользователя.

Результаты работ

В рамках проекта нам удалось достичь следующих результатов:

1. Получили доступ к базам данных с клиентскими документами.
2. Наладили надежный беспроводной доступ к внутренней сети компании.
3. Вошли в различные сервисы и системы компании из под скомпрометированных учетных записей сотрудников. Получили доступ к электронной почте, SharePoint, системе внутреннего документооборота, 1С КЭД и 1С ЗУП, Redash и другим системам.
4. Используя полученные привилегии в домене, получили доступ к системам резервного копирования. Однако из-за большого размера резервных копий их незаметная выгрузка из внутренней сети оказалась невозможной.

С точки зрения пентеста эти результаты можно считать успешными. Однако как Red Team мы выступили неудачно, ведь проект завершился раньше запланированного срока.

Результаты проверки работы службы реагирования

Пока мы работали, безопасники заказчика не сидели сложа руки. Они периодически выявляли подозрительные действия — блокировали сервисные аккаунты с доступом к чувствительной информации, меняли пароли ещё до наших попыток получить к ней доступ. Благодаря большому числу скомпрометированных учетных записей, мы могли продолжать работу, однако в определенный момент представитель заказчика сообщил, что мы раскрыты.

Первые подозрения вызвал наш Wi-Fi-адаптер. Вначале забыли сменить MAC-адрес, и при первом подключении он определялся как Alpha. Этот бренд ассоциируется с хакерами и привлек внимание при анализе логов.

Кроме того, команда допустила небрежность во время анализа данных. Один из наших пентестеров подключил к скомпрометированному почтовому ящику свой Outlook. Учетную запись ящика заблокировали, и все бы ничего, если бы не особенности работы Outlook. Если программа не может аутентифицироваться под заданной учетной записью, она пытается использовать текущую учетную запись Windows. Название учетки совпадало с ником нашего сотрудника на Хабре и в Telegram, что позволило отследить его связь с нашей компанией.

Наконец, была допущена ошибка при организации фишинговой атаки. При регистрации домена для отправки почты аккаунт назвали LLC Bastion. В случае пентеста это не имеет особого значения, но когда служба ИБ ККНН начала расследование и изучила письма в карантине, она окончательно раскрыла операцию. А ведь главное правило Red Team гласит: если тебя раскрыли — игра окончена.

…И другие интересные ошибки

Что касается других ошибок, то на старте команда набивала самые разные шишки.

Например, социальные инженеры не брали с собой оборудование для проведения атак на этапе разведки, что было вдвойне обидно в случаях, когда проникновение в офис заказчика было успешным. В другой раз, попав в корпоративную сеть в пятницу вечером, Red Team отправилась праздновать на выходные. За два дня Blue Team обнаружила атаку и заблокировала доступ, а новый мы так и не получили.

Эти ошибки имеют общие причины: инерция мышления и отсутствие привычки работать скрытно в условиях активного противодействия. Ведь в классических пентестах маскировка не требуется, тогда как в редтиминге из-за нее необходимо учитывать множество мелких деталей.

Специалисты Red Team постоянно балансируют между двумя задачами. С одной стороны, нужно не навредить инфраструктуре заказчика. С другой — обеспечить конфиденциальность своих действий. Это требует постоянного внимания и значительно увеличивает когнитивную нагрузку.

Поэтому редтиминг считается одним из самых сложных мероприятий в практике ИБ-команд. Но эта сложность и делает его привлекательным вызовом для многих профессионалов. Ради таких задач многие приходят в профессию.