



Тестирование корпоративных информационных систем на проникновение

Итоги внутренних пентестов — 2020

Содержание

Об исследовании	3
Ключевые цифры	3
Как мы получали контроль над инфраструктурой	4
Как мы получали доступ к бизнес-системам	12
Выводы и рекомендации	15

Об исследовании

В отчете представлены результаты работ по внутреннему тестированию на проникновение, которые были проведены специалистами Positive Technologies в 2019 году. Мы расскажем о распространенных недостатках защиты и методах атак, которые могут использовать злоумышленники, а также поделимся рекомендациями по повышению уровня защищенности.

Это продолжение исследования по результатам внешних пентестов, где рассматривались атаки от лица внешнего нарушителя. При проведении внутреннего пентеста моделируются атаки со стороны нарушителя, который находится внутри компании (например, атаки с типовым набором привилегий сотрудника или от лица случайного посетителя).

При внутреннем пентесте перед экспертами стоит задача определить максимально возможный уровень привилегий, который может получить злоумышленник. Дополнительно заказчик может ставить и другие задачи, например проверить возможность реализации кибератак на критически важные бизнес-системы. Цель тестирования на проникновение заключается в оценке эффективности используемых в компании средств защиты. Кроме того, во время пентеста можно оценить готовность служб ИБ к выявлению и пресечению атак, если они заранее не предупреждены о проводимых работах.

Для исследования были выбраны 23 проекта по внутреннему тестированию на проникновение — из числа проведенных в тех компаниях, которые разрешили использовать обезличенные данные. Мы учитывали только наиболее информативные проекты, чтобы объективно оценить защищенность корпоративной инфраструктуры.

Ключевые цифры

- В 2019 году получить полный контроль над инфраструктурой удалось во всех компаниях.
- На получение контроля над инфраструктурой требуется до пяти дней.
- В 61% компаний существует простой способ получить привилегии администратора домена, который под силу даже низкоквалифицированному хакеру.
- Почти половина всех действий пентестеров (47%) не отличаются от обычной деятельности пользователей или администраторов, а значит, и атака злоумышленника может остаться незамеченной.

Как мы получали контроль над инфраструктурой

В 2019 году нам удалось во всех компаниях получить полный контроль над инфраструктурой от лица внутреннего нарушителя. Как правило, на это уходило около трех дней, а в одной сети потребовалось всего 10 минут. В 61% компаний был выявлен хотя бы один способ получить контроль над инфраструктурой, сложность которого оценивалась как низкая.

Вектор атаки — это способ получения доступа к целевой системе в результате эксплуатации недостатков защищенности

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. В общем случае число шагов может равняться числу различных уязвимостей, которые нужно проэксплуатировать последовательно

Вектор атаки для получения привилегий администратора домена в среднем состоял из шести шагов. Однако большое количество шагов не всегда означает увеличение сложности. Во внутренней сети вектор обычно более длинный, чем при атаке из внешних сетей, потому что в процессе поиска учетной записи администратора домена необходимо перемещаться между значительным числом узлов.

Методы атак во внутренней сети основаны не только на эксплуатации уязвимостей ПО, но и на использовании архитектурных особенностей ОС и механизмов аутентификации, а также выполнении легитимных действий, предусмотренных функциональностью системы.

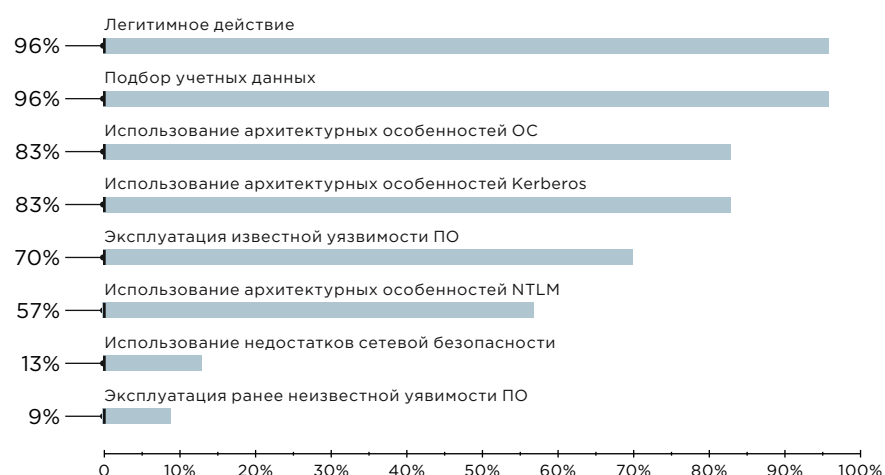


Рисунок 1. Успешные атаки (доли компаний)

Легитимные действия, которые позволяют развить вектор атаки, составили почти половину от всех действий пентестеров. К ним относятся, например, создание новых привилегированных учетных записей на узлах сети, создание дампа памяти процесса lsass.exe, выгрузка ветвей реестра, отправка запросов к контроллеру домена или клонирование виртуальных машин. Опасность состоит в том, что такие действия сложно отличить от обычной деятельности пользователей или администраторов, а значит, атака остается незамеченной.



Рисунок 2. Распределение успешных атак по категориям

Среди уязвимостей чаще всего выявлялись недостатки конфигурации, например отсутствие защиты служебных протоколов, недостаточная защита от восстановления учетных данных из памяти ОС, хранение важной информации в открытом виде. Каждой уязвимости присваивается уровень риска (критический, высокий, средний или низкий), который рассчитывается в соответствии с системой CVSS 3.1. Необходимо учитывать, что при проведении пентеста нет задачи выявить все уязвимости, существующие в системе. Цель работ заключается в получении объективной оценки уровня защищенности системы от атак со стороны внутренних нарушителей.

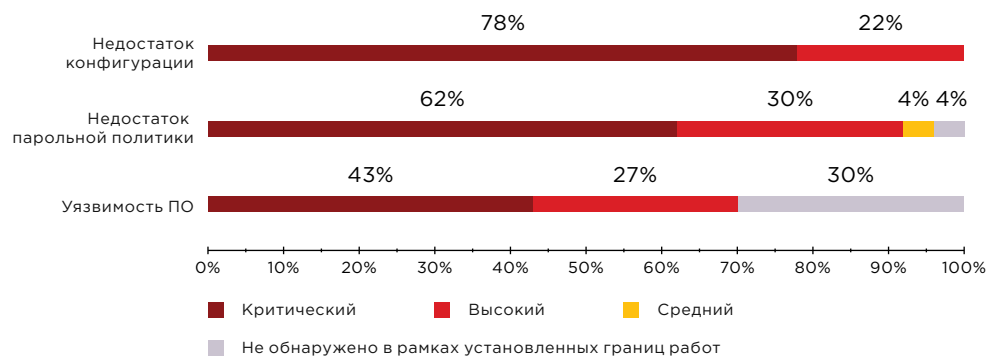


Рисунок 3. Максимальный уровень риска уязвимостей (доли компаний)

Как правило, вектор атаки строится на последовательном получении учетных данных пользователей и перемещении между узлами сети вплоть до обнаружения пароля администратора домена. Для поиска оптимального пути пентестеры используют программу Bloodhound, которое позволяет выявить связи между учетными записями и ресурсами домена, а также определить, в каких группах состоят пользователи.

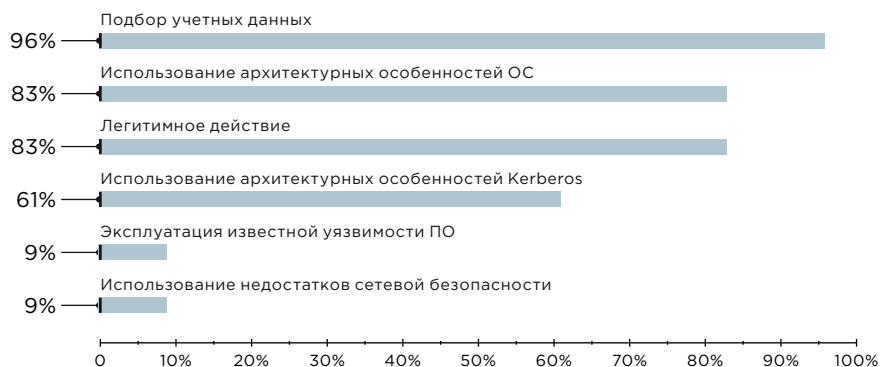


Рисунок 4. Успешные способы получения учетных данных (доли компаний)

Архитектурные особенности позволяют извлечь учетные данные из памяти ОС с помощью специальных утилит, таких как `mimikatz` и `secretsdump`, или используя встроенные средства ОС, например `taskmgr` для создания дампа процесса `lsass.exe`. Антивирусная защита не препятствовала созданию дампов памяти, только в одном проекте специалисты по ИБ получили уведомление о запуске утилиты `procdump`.

Рекомендации

Обеспечить защиту от восстановления учетных данных из памяти ОС. Рекомендуется использовать версии Windows выше 8.1 на рабочих станциях и версии Windows Server выше 2012 R2 на серверах. Привилегированных пользователей домена следует включить в группу `Protected Users`. На практике мы видим, что группа `Protected Users` редко используется для защиты привилегированных учетных записей, хотя применение такой техники способно значительно затруднить злоумышленнику развитие атаки.

В современных версиях Windows 10 и Windows Server 2016 реализована технология `Credential Guard`, позволяющая изолировать и защитить системный процесс `lsass.exe` от несанкционированного доступа.

Для дополнительной защиты привилегированных учетных записей, в частности администраторов домена, рекомендуется использовать двухфакторную аутентификацию. На архитектурном уровне для привилегированных пользователей рекомендуется организовать модель разграничения привилегий.

В 61% компаний успешно применялась атака `Kerberoasting`, которая основана на архитектурных особенностях Kerberos и направлена на получение учетных записей. Заключается она в следующем. Любой аутентифицированный в домене пользователь может запросить Kerberos-билет для доступа к сервису (TGS-REP), такой запрос является легитимным. При шифровании одной из частей билетов Kerberos TGS-REP используется NT-хеш пароля учетной записи, от имени которой запущен сервис, и этот пароль зачастую является

простым или словарным. Так как сервисные учетные записи могут иметь административные привилегии, то выполнив по словарю перебор паролей к полученным значениям Kerberos TGS-REP, злоумышленник может получить доступ к узлам с повышенными привилегиями. Подбор паролей проводится уже на компьютере атакующего, поэтому средствами защиты его не выявить. В одной из компаний в результате атаки Kerberoasting было получено около 4000 значений TGS-REP, а затем подобраны 25 паролей для выбранных привилегированных учетных записей.

```

/opt/tools/pentest/impacket/examples$ ./GetUserSPNs.py -request -dc-ip 10.10.10.10 10.10.10.10
Impacket v0.9.20-dev - Copyright 2019 SecureAuth Corporation

ServicePrincipalName      Name      MemberOf      PasswordLastSet      LastLogon
-----
...
$krb5tgs$

```

Рисунок 5. Получение значений TGS-REP с помощью атаки Kerberoasting

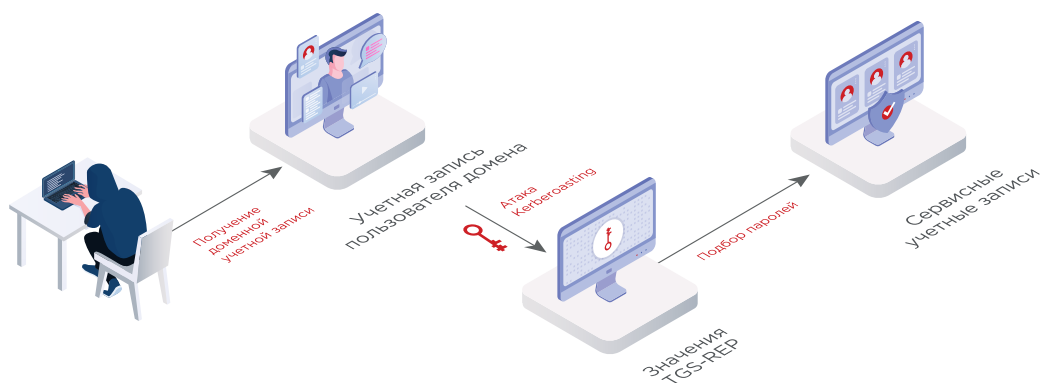


Рисунок 6. Получение сервисных учетных записей с помощью атаки Kerberoasting

Во многих компаниях из-за недостатков разграничения доступа произвольный пользователь домена может получить пароли локальных администраторов, назначенных службой Local Administrators Password Service, например подключившись к службе Active Directory домена с помощью утилиты Active Directory Explorer.

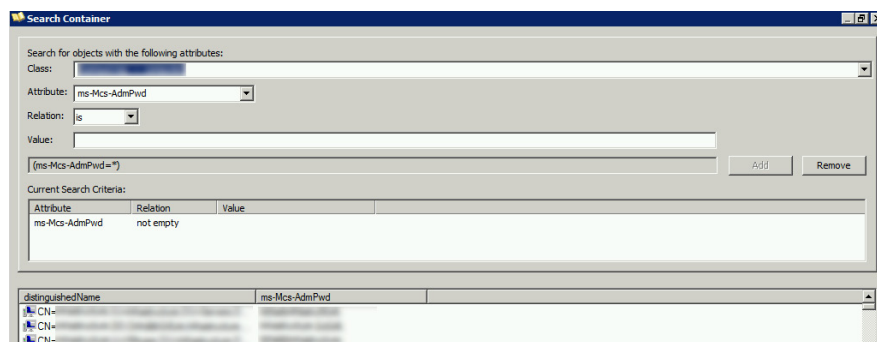


Рисунок 7. Получение паролей локальных администраторов

Рекомендации

Ограничить возможность получения учетных данных из LAPS для непривилегированных пользователей домена.

Те или иные недостатки защиты служебных протоколов были выявлены в 94% компаний, где проводился анализ сетевого трафика, однако в рамках пентестов атаки на эти протоколы проводятся редко, поскольку могут нарушить работу систем. Недостатки сетевой безопасности дают злоумышленнику возможность перехватить информацию, которая передается по сети, в том числе и учетные данные. К примеру, атака на протоколы LLMNR и NBNS позволяет получить идентификаторы пользователей и значения NetNTLMv2 challenge-response, по которым можно подобрать пароли с помощью утилиты hashcat.

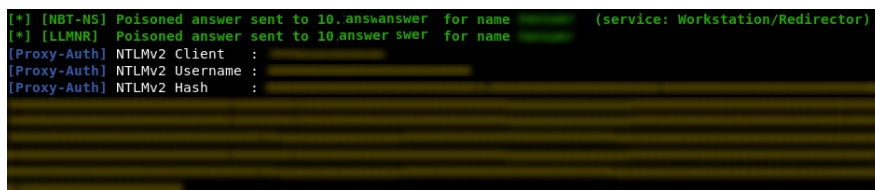


Рисунок 8. Перехват значений NetNTLMv2 challenge-response с помощью Responder

Рекомендации

По возможности отключить протоколы NBNS и LLMNR. Если использовать протокол NBNS необходимо — установить статические записи для основных узлов сети (шлюз по умолчанию, серверы), а также использовать WINS-сервер вместо широковещательных запросов. При использовании протокола LLMNR обеспечить его защиту, в частности не устанавливать его в качестве основного механизма для разрешения IP-адресов, а также ограничить область применения.

Практически в каждом проекте удавалось подобрать пароли пользователей (включая подбор по полученным вспомогательным данным, например NT-хешам или значениям TGS-REP). Самыми распространенными, даже среди привилегированных пользователей, оказались пароли, состоящие из сочетаний соседних символов на клавиатуре, например Qwerty123.

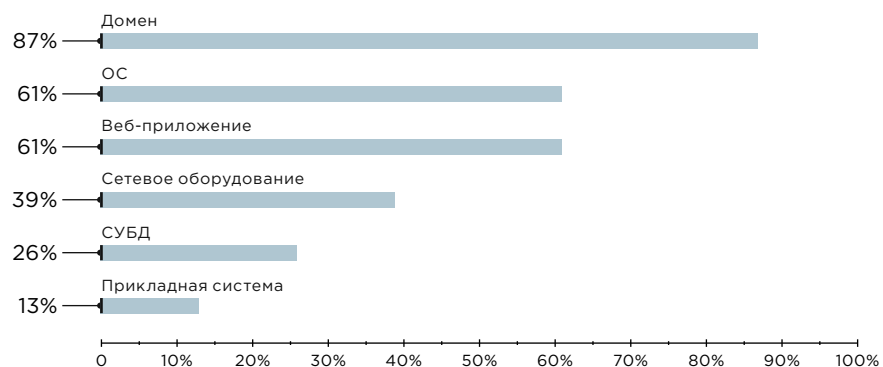


Рисунок 9. Где были выявлены ненадежные пароли (доли компаний)

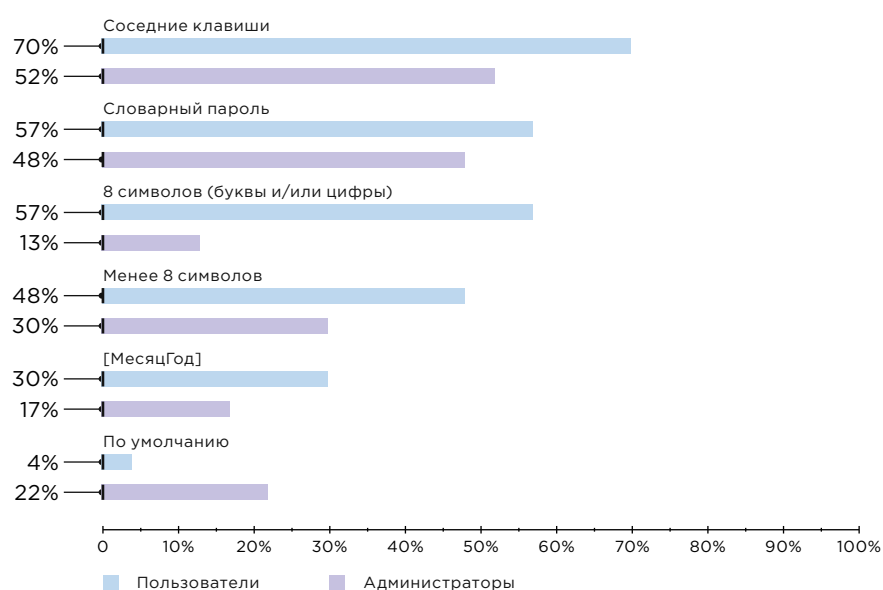


Рисунок 10. Распространенные типы паролей (доли компаний)

Самый простой вектор получения учетной записи администратора домена состоял всего из пары шагов. Сначала наши специалисты получили список идентификаторов всех пользователей домена с помощью команды `net user / domain`, а затем провели подбор учетных записей, которые используют пароль `Ltrf,hm2019` (Декабрь2019). Среди таких пользователей оказался и администратор домена.

Рекомендации

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

Проверять использование словарных паролей могут доменные администраторы — выгрузив файл `ntds.dit` с контроллера. В этом файле хранятся хеши паролей учетных записей всех пользователей домена. Можно в режиме офлайн попытаться подобрать по словарям пароли пользователей и в случае успешного подбора провести с соответствующими пользователями беседу, объяснить, почему важно сменить пароль на более стойкий. Такие мероприятия стоит проводить периодически.

Также следует рассмотреть возможность включения наиболее часто используемых паролей, которые публикуются в различных исследованиях по ИБ, в список запрещенных для использования в домене.

Архитектурные особенности протоколов NTLM и Kerberos активно использовались в атаках для перемещения между узлами сети, например с использованием известных техник `pass the hash`, `NTLM-relay`, `Kerberos silver ticket`, `Kerberos golden ticket`.

Злоумышленник может эксплуатировать известные уязвимости, которые содержатся в устаревших версиях ПО и позволяют удаленно выполнить произвольный код на рабочей станции, повысить привилегии или узнать важную информацию, например [CVE-2019-2725](#) в Oracle WebLogic, [CVE-2019-0686](#) в Microsoft Exchange Server, [CVE-2018-9276](#) в PRTG Network Monitor. Но чаще всего мы сталкиваемся с отсутствием актуальных обновлений ОС. Так, в Windows встречаются уязвимости [CVE-2019-0708](#) (BlueKeep), [CVE-2019-1040](#), а в некоторых компаниях до сих пор можно обнаружить уязвимости, которые были описаны в бюллетене безопасности [MS17-010](#) (в 30% компаний), и даже [MS08-067](#). При проведении работ были выявлены и две уязвимости нулевого дня.

В 22% компаний были получены привилегии не просто администратора домена, а администратора леса доменов (Enterprise Administrator). В частности, для этого проводилась атака `SID-History Injection`. Она заключается в следующем. Если домены `child.domain.local` и `domain.local` состоят в доверительных отношениях, то злоумышленник, имеющий максимальные привилегии в домене `child.domain.local`, может провести атаку, направленную на получение максимальных привилегий в корневом домене `domain.local`.

Domain trusts

CN	flatName	securityIdentifier	trustAttributes	trustDirection	trustType
...	...	S-1-	WITHIN_FOREST	BIDIRECTIONAL	UPLEVEL, MIT
...	...	S-1-	FOREST_TRANSITIVE	BIDIRECTIONAL	UPLEVEL, MIT
...	...	S-1-	WITHIN_FOREST	BIDIRECTIONAL	UPLEVEL, MIT
...	...	S-1-	WITHIN_FOREST	BIDIRECTIONAL	UPLEVEL, MIT
...	...	S-1-	FOREST_TRANSITIVE	BIDIRECTIONAL	UPLEVEL, MIT

Рисунок 11. Информация о доверительных отношениях домена

Атака основана на модификации атрибута sIDHistory, который предназначен для упрощения миграции доменов, например когда происходит слияние разных компаний или включение домена дочерней организации в домен головной компании. Когда требуется объединить в единую доменную инфраструктуру старый домен old.local с новым доменом new.local, все объекты домена old.local получают новые идентификаторы безопасности (SID) в домене new.local, а их старые значения SID записываются в атрибут sIDHistory. После объединения при аутентификации проверяется не только атрибут objectSid, но и sIDHistory. Для доменов, состоящих в доверительных отношениях, при междоменной аутентификации поле с атрибутом sIDHistory не фильтруется.

Внутри пакетов протокола Kerberos есть поле ExtraSids, в котором записано значение атрибута sIDHistory. Для проведения атаки требуется определить междоменный доверенный аккаунт, например с помощью утилиты LDAPPER, и получить NT-хеш его пароля. Используя полученный хеш пароля — сформировать Inter-Realm Ticket Granting Ticket (Inter-Realm TGT) с помощью утилиты ticketer. При этом в поле ExtraSids указывается значение SID корневого домена. Созданный Inter-Realm TGT используется для запроса Kerberos Silver Ticket для контроллера корневого домена.

```
$ python2 /opt/impacket/examples/ticketer.py -domain -domain-sid S-
-nthash -extra-sid S-
-500 -spn 'krbtgt/
Impacket v0.9.18-dev - Copyright 2018 SecureAuth Corporation

[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for
[*] PAC_LOGON_INFO
[*] PAC_CLIENT_INFO_TYPE
[*] EncTicketPart
[*] EncTGSRepPart
[*] Signing/Encrypting final ticket
[*] PAC_SERVER_CHECKSUM
[*] PAC_PRIVSVR_CHECKSUM
[*] EncTicketPart
[*] EncTGSRepPart
[*] Saving ticket in ccache
```

Рисунок 12. Создание Inter-Realm TGT

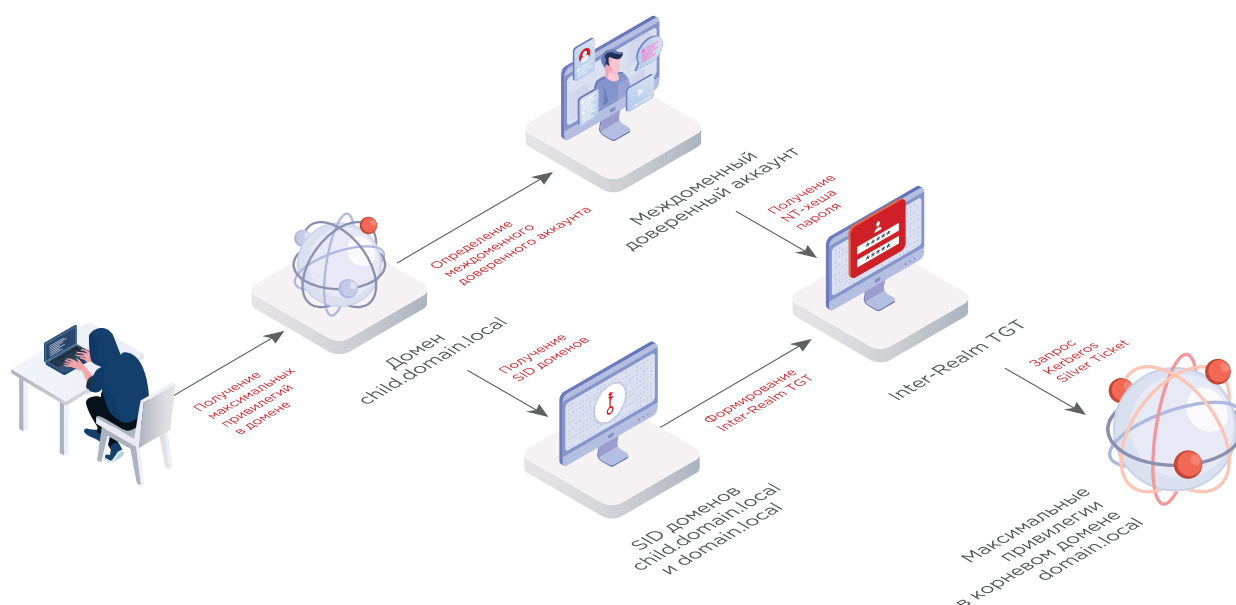


Рисунок 13. Получение максимальных привилегий в корневом домене

Рекомендации

Отключить опцию `sidHistory` для леса доменов, состоящих в доверительных отношениях. Также можно использовать опцию `SID Filter Quarantining` для доменов, состоящих в доверительных отношениях (атрибут `TREAT_AS_EXTERNAL`). Рекомендуется исключить недоверенные домены из леса и только затем настраивать для них фильтрацию `SID`.

Как мы получали доступ к бизнес-системам

В рамках внутреннего пентеста перед специалистами может стоять задача продемонстрировать возможность реализации бизнес-рисков или доступа к бизнес-системам. Для каждой компании перечень рисков будет отличаться, но есть и общие пункты, например компрометация критически важной информации в случае доступа к рабочим станциям руководства. Рассмотрим на нескольких примерах, как злоумышленники могут развить векторы атак.

Привилегии администратора домена позволяют злоумышленнику провести атаку `Kerberos Golden Ticket`. Протокол `Kerberos` основан на предоставлении билетов, подтверждающих уровень доступа пользователя к ресурсам доменной инфраструктуры. Привилегии служебной учетной записи `krbtgt` позволяют выпустить билет с любым уровнем доступа. Поэтому нарушитель, который может получить NT-хеш учетной записи `krbtgt`, в том числе администратор домена, имеет возможность создать «золотой билет» (`Golden Ticket`) для доступа к ресурсам с любыми привилегиями.

Чтобы устранить последствия атаки `Kerberos Golden Ticket` необходимо дважды сменить пароль учетной записи `krbtgt`, а также провести расследование инцидента и переустановить системы на скомпрометированных узлах.

С помощью атаки `Golden Ticket` злоумышленник может подключиться к компьютеру топ-менеджера и установить ПО для скрытого удаленного доступа, например модифицированную версию `TeamViewer` или `VNC`, — и незаметно наблюдать за всеми действиями пользователя.

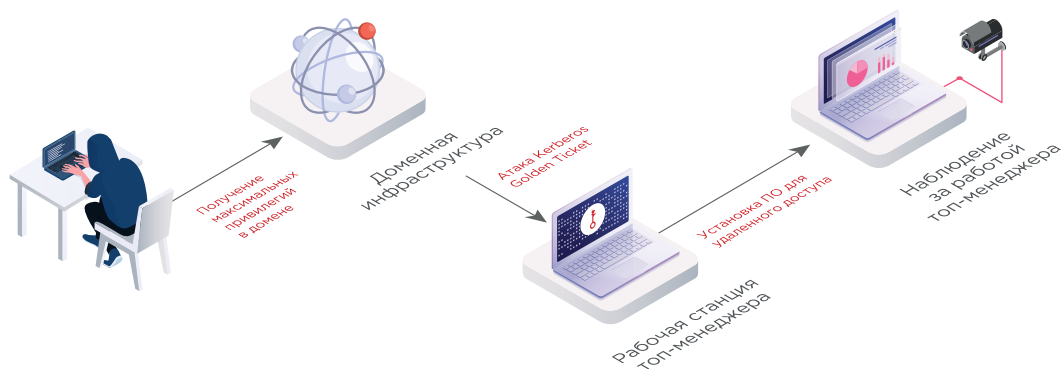


Рисунок 14. Вектор атаки для доступа к рабочей станции топ-менеджера

Рассмотрим другой пример. В ходе внутреннего пентеста был установлен адрес терминального сервера, с которого сотрудники подключались к системе TranzWare Online для управления сетью банкоматов. Поскольку пентестеры уже обладали привилегиями администратора домена, они смогли провести атаку Golden Ticket для доступа к серверу. Затем они создали дампы памяти процесса lsass.exe и с помощью утилиты mimikatz извлекли пароли пользователей в открытом виде. Подключившись к серверу уже с полученными учетными данными, специалисты выяснили, что для доступа к TranzWare Online используются те же пароли, что и для доменных учетных записей, и продемонстрировали возможность авторизации в системе. В результате такой атаки злоумышленник смог бы управлять конфигурацией банкоматов, просматривать список транзакций и иную отчетность на банкомате, а также попытаться провести мошеннические транзакции и похитить деньги.

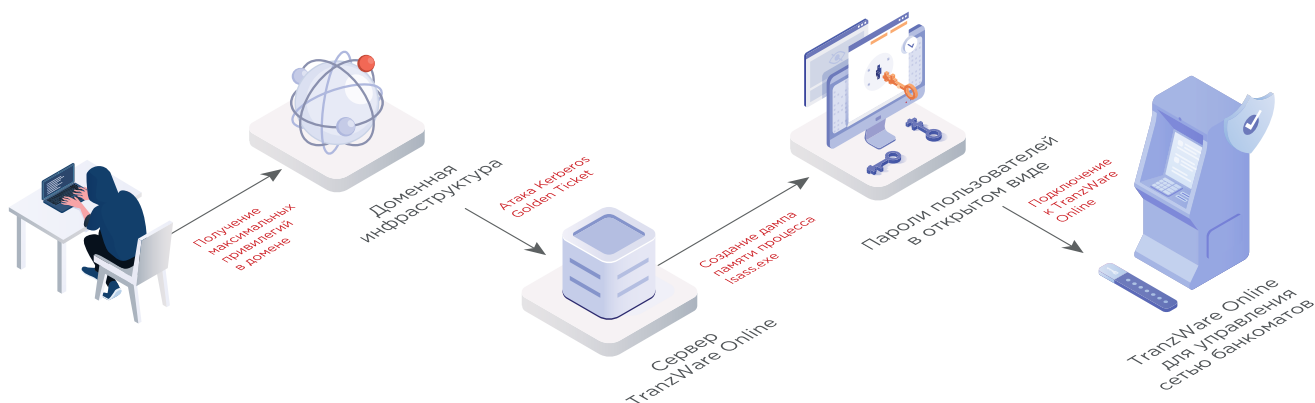


Рисунок 15. Вектор атаки на сеть банкоматов

Промышленным и топливно-энергетическим компаниям важно проверять уровень защищенности технологической сети. На практике оказывается, что из корпоративного сегмента злоумышленник может проникнуть в технологический. Приведем пример такого вектора атаки.

Во время пентеста на одном из узлов сети был создан дамп памяти процесса lsass.exe, из которого были извлечены несколько учетных записей. Анализ доменной инфраструктуры с помощью программы Bloodhound показал, что одна из этих учетных записей обладает привилегиями локального администратора на множестве узлов сети. Пентестеры изучили сведения о сотрудниках на корпоративном портале и с помощью полученной привилегированной учетной записи подключились к рабочим станциям пользователей, предположительно имеющих доступ к автоматизированным системам управления. На одной из рабочих станций они обнаружили информацию о технологической сети, способах подключения к промышленным системам и учетные данные.

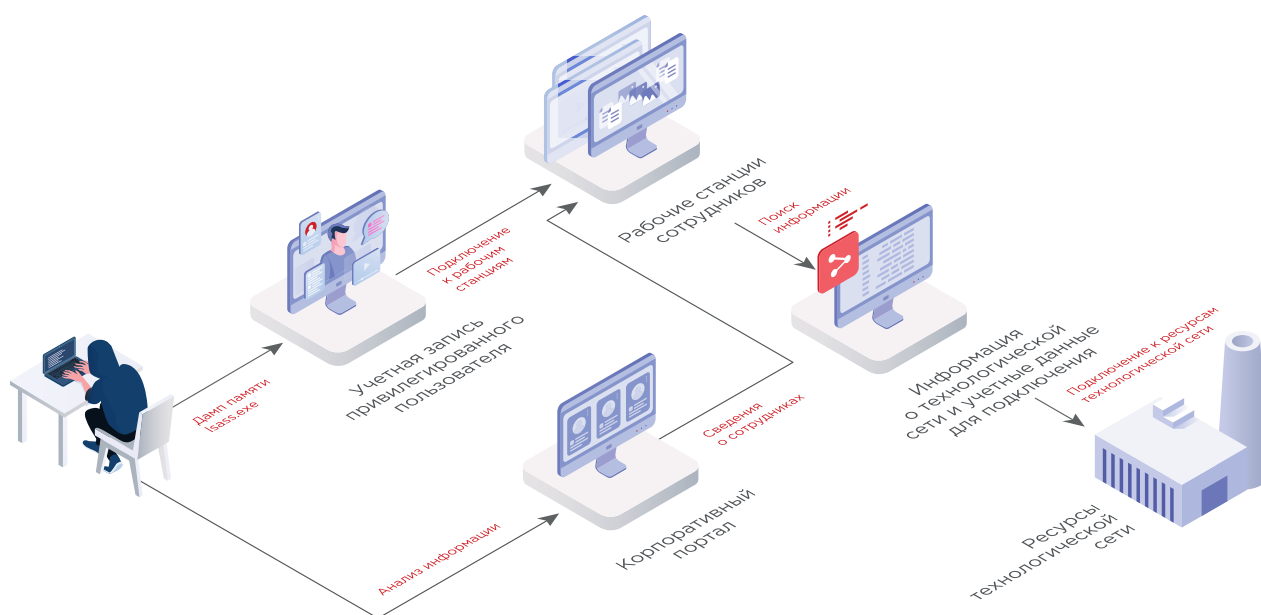


Рисунок 16. Вектор атаки на ресурсы технологической сети

Выводы и рекомендации

Тестирование корпоративных информационных систем на проникновение традиционно показывает низкий уровень защищенности от внутреннего нарушителя, который может получить полный контроль над инфраструктурой и доступ к критически важным бизнес-системам. По большей части атаки возможны из-за недостатков конфигурации и слабой парольной политики, поэтому в первую очередь необходимо соблюдать базовые правила информационной безопасности. Рекомендации по защите от распространенных методов атак приведены в исследовании.

Действия пентестеров редко привлекали к себе внимание, а следовательно, и злоумышленники могли бы долгое время скрытно находиться в инфраструктуре. Так, в ходе работ по внешнему тестированию на проникновение выявлялись следы более ранних атак хакеров, которые не были вовремя замечены службой ИБ. Важно использовать современные технические решения, которые дают возможность на ранней стадии обнаружить попытки атак. Системы анализа и мониторинга событий безопасности (SIEM-системы) позволяют выявить подозрительную активность в инфраструктуре и принять меры по пресечению атак, чтобы минимизировать негативные последствия. Помимо этого, рекомендуется регулярно проводить ретроспективный анализ событий безопасности и трафика внутри сети, чтобы обнаружить присутствие злоумышленников, если система все же была взломана. Средства глубокого анализа сетевого трафика позволяют не только выявить факт компрометации, но и отследить действия нарушителей в инфраструктуре. Своевременное выявление атаки дает возможность остановить ее до того, как будет нанесен серьезный ущерб компании, минимизировать риски кражи конфиденциальной информации, нарушения бизнес-процессов и финансовых потерь.

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

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](#).