СЦЕНАРИИ ДЛЯ ВЗЛОМА

Евгений Кецкер
Старший инженер
Компания «Инфосистемы Джет»
Сергей Ковалев
Ведущий инженер
Компания «Инфосистемы Джет»

РАЗБИРАЕМ ТИПОВЫЕ СЦЕНАРИИ АТАК НА КОРПОРАТИВНЫЕ СЕТИ

Пионистеры Positive Technology ежегодно выполняют десятистраничный на проникновение для крупнейших компаний в России и за рубежом. Для отчета о работах, которые готовящим отчет, эксперты, которые использовали при проведении компаний и сообщили [читать полный](#) [лист](#) [заказчика](#) в 80% случаев.

ПАРО

Что нужно рассказать здесь рассуждения и мне по отношению выполненному аналитику? Сразу отмечаем сценарии для не приемлемо с через достаточно. Необходимо выделить защиты могут встречаться в любой отрасли и заинтересованных сторон.

ПРОДОЛЖЕНИЕ ПЕРИМЕТРА

Что касается внешнего периметра, нарушить должны получить доступ к сети, подключенной также к внешнему периметру. Для этого злоумышленнику необходимо выполнить следующие действия:

- недостаточно управляемые учетные записи;
- недостаточно управляемые;
- недостаточно управляемые;
- недостаточно управляемые;
- недостаточно управляемые;
- отсутствие обновлений;
- плохие конфигурирования, плохие конфигурирования, плохие конфигурирования,

СЦЕНАРИИ ДЛЯ ВЗЛОМА

РАЗБОРКИ ТИПОВЫХ СЦЕНАРИЕВ АТАК НА КОРПОРАТИВНЫЕ СЕТИ

Сценарий 4. Социальные инженерии

Сценарий 4. Социальные инженерии. Данные распространяются методом «почтовые вирусы», которые могут использовать исключительно отечественные сервисы и которым бесполезны. Нарушитель может извлекать данные для другого сценария, а также использовать для шифрования данных в «плохом».

Примеры: первый сценарий «почтовые вирусы» в телефонах (регистрация одного из работников банка сопровождалась перехлестом которого нам удалось перехватить). Второй сценарий «плохой» — в ноутбуке сотрудника крупной компании (рассмотрим ниже). Это был один из тех случаев, когда не просто перешли по ссылке из письма, а еще и встроили в переписку с сотрудником, который ждал ссылку, и сделали ее «правильной» для сотрудника этого.

Для сотрудника на увеличение социальных гарантий

Ниже сценарий «плохого» — в ноутбуке сотрудника крупной компании (рассмотрим ниже). Это был один из тех случаев, когда не просто перешли по ссылке из письма, а еще и встроили в переписку с сотрудником, который ждал ссылку, и сделали ее «правильной» для сотрудника этого.

Ни разу сценарий «плохого» не сработал, несмотря на «плохие» данные. Сценарий «плохого» — в ноутбуке сотрудника крупной компании. Здесь также бывалые, но все сотрудники занимают крупные должности, и «плохие» данные могут использовать для перехватывания. Адреса были подобраны отрасленьтальности, которая сотрудничает с крупными компаниями, а также с крупными компаниями, которые сотрудничают. Вторично, «плохие» подарки и «гарантии» были.

Уважаемые коллеги!
Уважаемые коллеги!
Уважаемые коллеги!

СЦЕНАРИИ ДЛЯ ВЗЛОМА

ПОТРЕБИТЕЛЬСКИЕ СЕРВИСЫ НА КОРПОРАТИВНЫЕ СЕТИ

Сценарий 2. Атака на протоколы сетевого и канального уровней

Если подобрать сильные пароли не удалось или есть сомнения на счет надежности шифрования, то можно попробовать атаковать протоколы сетевого и канального уровней. Для этого необходимо иметь доступ к сетевому трафику пользователя и уметь его перехватывать. В частности, он может передавать клиент-серверные или peer-to-peer-сообщения, которые, в свою очередь, могут быть использованы для получения информации о наших предполагаемых жертвах.

Для перехвата трафика можно использовать, например, утилиту Ettercap. Ettercap — это свободно распространяемый сетевой анализатор трафика с поддержкой перехвата и модификации трафика в реальном времени. Ettercap поддерживает перехват как для сетевых, так и для канальных протоколов, а также для протоколов шифрования SSH и HTTPS.

В результате этой атаки можно получить доступ к сетевому оборудованию, к ресурсам корпоративной сети, к почтовым ящикам, к ресурсам, которые могут быть использованы, причем или без доступа к системе.

Протоколы NetBIOS Name Service (NBNS) и LLMNR (Link Multicast Name Resolution) LLMNR, используется для установления IP-адреса узла в том случае, если DNS-сервер не может определить IP-адрес по имени узла. Если DNS-сервер не может определить IP-адрес по имени узла, то клиентский компьютер посылает сообщение в сеть с запросом на определение IP-адреса. Если в ответ на запрос не приходит ответ, то клиентский компьютер посылает сообщение в сеть с запросом на определение IP-адреса по протоколу NBNS. Если в ответ на запрос приходит ответ, то клиентский компьютер посылает запрос на получение ресурсов по протоколам SMB и NetBIOS.

Получив адресованный этим узлам запрос, клиентский компьютер посылает сообщение с запросом на получение ресурсов по протоколам SMB и NetBIOS.

Ettercap поддерживает этот атаки в случае сетевого трафика учетных данных корпоративной сети. Для этого необходимо иметь доступ к сетевому трафику корпоративной сети и уметь обходить применяемые в корпоративной сети средства обнаружения сетевых атак, например, IDS/IPS.

Рекомендации по защите. Если в корпоративной сети используются протоколы, то на сервере отключить. Если же они нужны, то проверить, сколько клиентов в сети использует эти протоколы. Если клиентов не больше 10, то можно отключить протоколы на клиентских компьютерах. В противном случае, если в сети есть WINS-сервер, можно настроить отключение WINS-клиентов. Если WINS-сервер отсутствует, то можно использовать файл LMHOSTS для ограничения доступа к ресурсам. Для ограничения доступа к ресурсам можно использовать файлы HOSTS. Если в сети есть Active Directory, можно использовать DNS-сервер.

Сценарий 3. Атака SMB Relay

Если в сети используются протоколы NBNS и LLMNR, то атакующий может использовать для получения доступа к ресурсам корпоративной сети уязвимость протокола SMB. Для этого необходимо иметь доступ к сетевому трафику корпоративной сети. Для получения доступа к ресурсам корпоративной сети можно использовать утилиту Responder. Responder — это свободно распространяемый сетевой анализатор трафика, который поддерживает перехват учетных данных по протоколам SMB, NBNS, LLMNR и прокси-серверов WPAD. Responder может использовать для получения доступа к ресурсам корпоративной сети уязвимость протокола SMB.

Пример атаки SMB Relay:

На атакованном сервере возможно выполнение команды с привилегиями того пользователя, чьи учетные данные были перехвачены. Для выполнения команды на атакованном сервере можно использовать утилиту psexec.exe. Для выполнения команды на атакованном сервере можно использовать утилиту psexec.exe.

Перечислить ресурсы корпоративной сети можно. В частности, сетевые анализаторы могут использовать для получения информации о сетевом трафике, а также сканеры, которые, в отличие обнаружения уязвимостей, могут использовать для получения информации о ресурсах корпоративной сети. Для получения информации о ресурсах корпоративной сети можно использовать утилиту Nmap.

Рекомендации по защите. Для защиты от атаки на корпоративные ресурсы необходимо использовать IDS/IPS, которые могут обнаружить сканирование ресурсов корпоративной сети.

Сценарий 4. Получение конфиденциальной информации

Если в корпоративной сети используются протоколы, которые используют для аутентификации пароли, то можно попытаться перехватить пароли. Для перехвата паролей можно использовать утилиту Responder.

Рекомендации по защите. Для защиты от атаки на корпоративные ресурсы необходимо использовать IDS/IPS, которые могут обнаружить попытки получения паролей.

Сценарий 5. Получение значимых данных

Если сценарии атаки на протоколы сетевого и канального уровней не дали результата, то можно попытаться атаковать прикладные протоколы. Для перехвата трафика прикладных протоколов можно использовать утилиту Ettercap. Ettercap поддерживает перехват как для сетевых, так и для канальных протоколов, а также для протоколов шифрования SSH и HTTPS.

В результате атаки на прикладные протоколы можно получить доступ к ресурсам корпоративной сети, к почтовым ящикам, причем или без доступа к системе.

Перехватить пароли можно с помощью утилиты ettercap. В частности, сетевые анализаторы могут использовать для получения информации о сетевом трафике, а также сканеры, которые, в отличие обнаружения уязвимостей, могут использовать для получения информации о ресурсах корпоративной сети. Для получения информации о ресурсах корпоративной сети можно использовать утилиту Nmap.

Рекомендации по защите. Для защиты от атаки на корпоративные ресурсы необходимо использовать IDS/IPS, которые могут обнаружить попытки получения паролей.

Сценарий 6. Получение значимых данных

Если сценарии атаки на протоколы сетевого и канального уровней не дали результата, то можно попытаться атаковать прикладные протоколы. Для перехвата трафика прикладных протоколов можно использовать утилиту Ettercap. Ettercap поддерживает перехват как для сетевых, так и для канальных протоколов, а также для протоколов шифрования SSH и HTTPS.

В результате атаки на прикладные протоколы можно получить доступ к ресурсам корпоративной сети, к почтовым ящикам, причем или без доступа к системе.

Перехватить пароли можно с помощью утилиты ettercap. В частности, сетевые анализаторы могут использовать для получения информации о сетевом трафике, а также сканеры, которые, в отличие обнаружения уязвимостей, могут использовать для получения информации о ресурсах корпоративной сети. Для получения информации о ресурсах корпоративной сети можно использовать утилиту Nmap.

Рекомендации по защите. Для защиты от атаки на корпоративные ресурсы необходимо использовать IDS/IPS, которые могут обнаружить попытки получения паролей.

Сценарий 7. Получение значимых данных

Если сценарии атаки на протоколы сетевого и канального уровней не дали результата, то можно попытаться атаковать прикладные протоколы. Для перехвата трафика прикладных протоколов можно использовать утилиту Ettercap. Ettercap поддерживает перехват как для сетевых, так и для канальных протоколов, а также для протоколов шифрования SSH и HTTPS.

В результате атаки на прикладные протоколы можно получить доступ к ресурсам корпоративной сети, к почтовым ящикам, причем или без доступа к системе.

Перехватить пароли можно с помощью утилиты ettercap. В частности, сетевые анализаторы могут использовать для получения информации о сетевом трафике, а также сканеры, которые, в отличие обнаружения уязвимостей, могут использовать для получения информации о ресурсах корпоративной сети. Для получения информации о ресурсах корпоративной сети можно использовать утилиту Nmap.

Рекомендации по защите. Для защиты от атаки на корпоративные ресурсы необходимо использовать IDS/IPS, которые могут обнаружить попытки получения паролей.

Сценарий 8. Получение значимых данных

Если сценарии атаки на протоколы сетевого и канального уровней не дали результата, то можно попытаться атаковать прикладные протоколы. Для перехвата трафика прикладных протоколов можно использовать утилиту Ettercap. Ettercap поддерживает перехват как для сетевых, так и для канальных протоколов, а также для протоколов шифрования SSH и HTTPS.

В результате атаки на прикладные протоколы можно получить доступ к ресурсам корпоративной сети, к почтовым ящикам, причем или без доступа к системе.

Перехватить пароли можно с помощью утилиты ettercap. В частности, сетевые анализаторы могут использовать для получения информации о сетевом трафике, а также сканеры, которые, в отличие обнаружения уязвимостей, могут использовать для получения информации о ресурсах корпоративной сети. Для получения информации о ресурсах корпоративной сети можно использовать утилиту Nmap.

Рекомендации по защите. Для защиты от атаки на корпоративные ресурсы необходимо использовать IDS/IPS, которые могут обнаружить попытки получения паролей.

Сценарий 9. Получение значимых данных

Если сценарии атаки на протоколы сетевого и канального уровней не дали результата, то можно попытаться атаковать прикладные протоколы. Для перехвата трафика прикладных протоколов можно использовать утилиту Ettercap. Ettercap поддерживает перехват как для сетевых, так и для канальных протоколов, а также для протоколов шифрования SSH и HTTPS.

В результате атаки на прикладные протоколы можно получить доступ к ресурсам корпоративной сети, к почтовым ящикам, причем или без доступа к системе.

Перехватить пароли можно с помощью утилиты ettercap. В частности, сетевые анализаторы могут использовать для получения информации о сетевом трафике, а также сканеры, которые, в отличие обнаружения уязвимостей, могут использовать для получения информации о ресурсах корпоративной сети. Для получения информации о ресурсах корпоративной сети можно использовать утилиту Nmap.

Рекомендации по защите. Для защиты от атаки на корпоративные ресурсы необходимо использовать IDS/IPS, которые могут обнаружить попытки получения паролей.

Сценарий 10. Получение значимых данных

Если сценарии атаки на протоколы сетевого и канального уровней не дали результата, то можно попытаться атаковать прикладные протоколы. Для перехвата трафика прикладных протоколов можно использовать утилиту Ettercap. Ettercap поддерживает перехват как для сетевых, так и для канальных протоколов, а также для протоколов шифрования SSH и HTTPS.

В результате атаки на прикладные протоколы можно получить доступ к ресурсам корпоративной сети, к почтовым ящикам, причем или без доступа к системе.

Перехватить пароли можно с помощью утилиты ettercap. В частности, сетевые анализаторы могут использовать для получения информации о сетевом трафике, а также сканеры, которые, в отличие обнаружения уязвимостей, могут использовать для получения информации о ресурсах корпоративной сети. Для получения информации о ресурсах корпоративной сети можно использовать утилиту Nmap.

Рекомендации по защите. Для защиты от атаки на корпоративные ресурсы необходимо использовать IDS/IPS, которые могут обнаружить попытки получения паролей.

Сценарий 11. Получение значимых данных

Если сценарии атаки на протоколы сетевого и канального уровней не дали результата, то можно попытаться атаковать прикладные протоколы. Для перехвата трафика прикладных протоколов можно использовать утилиту Ettercap. Ettercap поддерживает перехват как для сетевых, так и для канальных протоколов, а также для протоколов шифрования SSH и HTTPS.

В результате атаки на прикладные протоколы можно получить доступ к ресурсам корпоративной сети, к почтовым ящикам, причем или без доступа к системе.

Перехватить пароли можно с помощью утилиты ettercap. В частности, сетевые анализаторы могут использовать для получения информации о сетевом трафике, а также сканеры, которые, в отличие обнаружения уязвимостей, могут использовать для получения информации о ресурсах корпоративной сети. Для получения информации о ресурсах корпоративной сети можно использовать утилиту Nmap.

Рекомендации по защите. Для защиты от атаки на корпоративные ресурсы необходимо использовать IDS/IPS, которые могут обнаружить попытки получения паролей.

ЗАКЛЮЧЕНИЕ

Перечисленные сценарии атак — лишь часть так называемых, что используются для получения доступа к корпоративным ресурсам. Для каждого из сценариев можно использовать несколько утилит.

Перед атакой сценария обычно выполняется предварительная атака, которая позволяет определить, какие сценарии атаки можно использовать. Для определения сценариев атаки можно использовать утилиту Nmap. Для определения сценариев атаки можно использовать утилиту Nmap. Для определения сценариев атаки можно использовать утилиту Nmap