БЮЛЛЕТЕНЬ

Защита от атак класса MITM, Sniffing, Relay

Контакты:

info@axxtel.ru

+7 (383) 255-3-255

Внимание! Текущие рекомендации не учитывают особенностей каждой инфраструктуры сети и могут привести к отказу работоспособности систем, работающих на основе устаревших протоколов. Не рекомендуется применять данные рекомендации без предварительного тестирования и анализа возможных последствий.

Рекомендации по защите от атак ARP Poisoning

Процесс преобразования IP в MAC-адреса по протоколу ARP имеет ряд уязвимостей, которыми может воспользоваться злоумышленник:

- ARP – это протокол без сохранения состояния. Сетевые узлы автоматически кэшируют все полученные ответы ARP.
- Сетевые узлы кэшируют ответы ARP, даже если они не были запрошены.
- Новые ответы ARP заменяют предыдущие.
- Протокол ARP не имеет метода проверки содержимого ответа ARP.

Злоумышленник может выдать себя за другой хост в сети, отправив поддельный ответ ARP по сети. Поддельный ARP-ответ будет содержать реальный MAC-адрес злоумышленника и IP-адрес жертвы. Широковещательная передача будет связывать физический MAC-адрес злоумышленника с IP-адресом жертвы благодаря механизму кэширования ответов ARP. Таким образом, хосты будут подвержены манипуляциям с трафиком, которые могут передавать их данные о трафике злоумышленнику, а не реальному хосту. По этой причине злоумышленники могут контролировать трафик в сети.

Защититься от атаки ARP Poisoning можно несколькими способами:

1. *Использование фильтрации пакетов.* Фильтрация пакетов позволяет идентифицировать и перехватывать пакеты до того, как они достигнут получателя. Пакеты, которые конфликтуют с исходной информацией, будут отбрасываться.
2. *Использование статического ARP.* Настройка статического ARP предотвратит кэширование ARP на узлах сети. Его можно настроить на коммутаторах, которые привяжут MAC-адреса к определенным портам.
3. *Использование Dynamic ARP Inspection (DAI).* Dynamic ARP Inspection (DAI) – это функция безопасности, которая позволяет сетевому устройству проверять на соответствие MAC-адреса и IP-адреса на не доверенных портах.
4. *Использование Security Endpoint Protection на антивирусных средствах защиты.* Некоторые антивирусы позволяют обнаруживать подозрительную активность в сети, наблюдая за изменениями в локальном кэше ARP и сетевым трафиком.
5. *Использование криптографических протоколов.* TLS, SSL, SSH и другие протоколы, использующие криптографию, минимизируют риск кражи конфиденциальной информации в случае атак ARP Poisoning.

Рекомендации по защите от атак DHCP Spoofing

Злоумышленник может выполнить комбинацию атак – DHCP Starvation и DHCP Spoofing, чтобы запустить атаку Man-In-The-Middle. Атака DHCP Starvation происходит, когда злоумышленник отправляет несколько сообщений DHCP REQUEST с поддельными исходными MAC-адресами. Затем злоумышленник может настроить мошеннический DHCP-сервер и отвечать на новые DHCP-запросы своими собственными сетевыми настройками, имитируя шлюз по умолчанию и DNS-сервер.

Стоит упомянуть отдельный случай, когда в сети включен и не настроен протокол IPv6, являющийся для ОС Windows по умолчанию более приоритетным, чем IPv4. В таких случаях злоумышленнику не обязательно проводить атаку DHCP Starvation – ему достаточно представиться сервером DHCPv6, который будет приоритетнее легитимного сервера DHCPv4.

Для защиты от DHCP Spoofing используйте решение DHCP Snooping. В случае неиспользования протокола IPv6 рекомендуется отключить его на клиентских устройствах с ОС Windows.

DHCP Snooping представляет собой набор различных комбинированных методов, направленных на снижение и смягчение воздействия атак с подменой DHCP.

Большинство современных коммерческих продуктов и оборудования предлагают простые в настройке (или даже не требующие настройки) надстройки и параметры отслеживания DHCP. Проконсультируйтесь с производителями сетевого оборудования, чтобы внедрить такие быстрые и эффективные решения.

DHCP Snooping можно настроить на коммутаторах LAN для предотвращения вредоносного или искаженного трафика DHCP или мошеннических серверов DHCP.

Другие функции могут использовать информацию базы данных отслеживания DHCP. Эта информация позволяет:

- Убеждаться, что хосты используют только назначенные им IP-адреса в сочетании с source-guard.
- Осуществлять обработку запросов ARP в сочетании с arp-Inspection.
- Отбрасывать сообщения DHCP с ненадежного DHCP-сервера. Надежные DHCP-серверы идентифицируются путем настройки состояния доверия для отслеживания DHCP порта коммутатора. Сообщения DHCP-сервера могут проходить через порты коммутаторов, которые находятся в доверенном состоянии DHCP-отслеживания.

Сообщения DHCP-сервера будут отброшены при попытке пройти через порт коммутатора, которому не доверяют.

- Отбрасывать сообщения DHCP, если исходный MAC-адрес и MAC-адрес встроенного клиентского оборудования не совпадают. Однако при плохо написанной реализации IP-поставщика эту защиту можно обойти. Наиболее распространенным сценарием является переадресация запроса DHCP между интерфейсами на одном и том же устройстве.
- Отбрасывать сообщения, которые отменяют аренду или отклоняют предложение, если сообщение об освобождении или отклонении получено на порту коммутатора, отличном от порта, на котором был проведен исходный диалог DHCP. Это предотвращает прекращение аренды или отклонение предложения DHCP третьей стороной от имени реального клиента DHCP.

Дополнительные ресурсы:

- https://www.juniper.net/documentation/en_US/junos/topics/task/verification/port-security-dhcp-snooping.html
- http://www.pearsonitcertification.com/articles/article.aspx?p=2474170

Рекомендации по защите от атак LLMNR/NBNS Poisoning

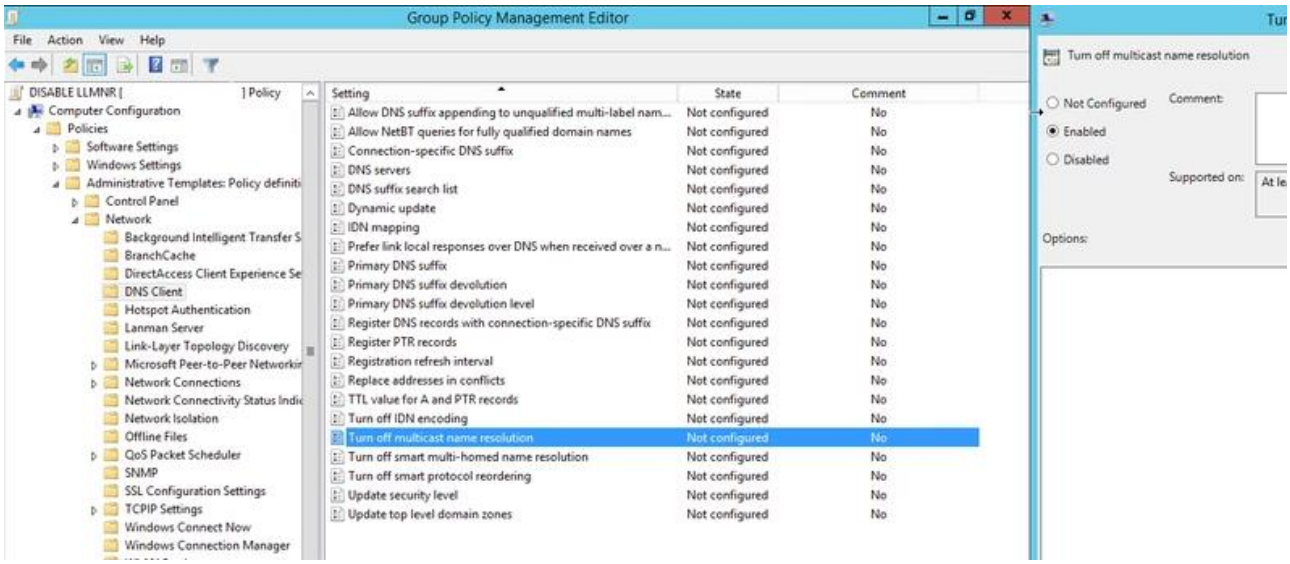
LLMNR (Link-Local Multicast Name Resolution), NBNS (Netbios Name Service) и mDNS (Multicast Domain Name Service) – это протоколы Microsoft Windows, служащие альтернативными методами разрешения имен. Если машина пытается разрешить конкретный хост, но разрешение DNS не удается, машина попытается запросить правильный адрес через LLMNR, NBNS или mDNS у всех других машин в локальной сети. Поскольку эта операция выполняется с использованием широковещательных или многоадресных запросов без средств проверки, она подвержена злонамеренным ответам, распространяющимся злоумышленниками.

Рекомендуется отключить эти протоколы. Это можно сделать следующим образом:

Отключение LLMNR с помощью GPO:

1. Создайте новую запись GPO для всех компьютеров в среде.
2. Перейдите к «Политика локального компьютера / Конфигурация компьютера / Административные шаблоны / Сеть / DNS-клиент».

3. Установите для параметра «Turn off multicast name resolution» значение «Enabled».



Отключение NBNS в случае использования среды DHCP:

1. Перейти к управлению DHCP.
2. Перейдите в «Scope options» для изменяемой сети.
3. Щелкните правой кнопкой мыши и настройте параметры.
4. Выберите вкладку «Advanced» и измените «Vendor class» на «Microsoft Options».
5. Во фрейме «Available options» установите флажок «001 Microsoft Disable Netbios Option».
6. Во фрейме «Data Entry» измените запись данных на 0x2.
7. Щелкните "ОК". Новые настройки вступят в силу, когда клиенты обновят свои адреса.

Отключение NBNS для одного компьютера:

1. Откройте «Панель управления».
2. Откройте «Центр управления сетями и общим доступом».
3. Нажмите «Изменить настройки адаптера».
4. Щелкните правой кнопкой мыши на «Подключение по локальной сети» и выберете «Свойства».
5. Дважды щелкните на «Протокол IPv4».

6. Нажмите «Дополнительно», а затем перейдите во вкладку «WINS».
7. Щелкните «Отключить NetBIOS через TCP/IP».

Рекомендации по защите от атак SMB Relay

Сообщения SMB могут использоваться злоумышленниками двумя способами:

1. *Атака Man-In-The-Middle*: Злоумышленник может отравить сеть и заставить жертву отправить SMB-запрос на свой компьютер. Далее этот запрос будет перенаправлен злоумышленником на целевой компьютер с ОС Windows. После завершения перенаправления запроса злоумышленник, желая использовать сообщение для запуска вредоносного кода на целевой машине, использует аутентификацию жертвы.

2. *Обновление настроек организации, например, GPO*: Поскольку протокол SMB используется для отправки команд и обновлений, например, групповой политики организации, злоумышленник, желая снизить параметры безопасности организации, может захватить сообщение и обновить его.

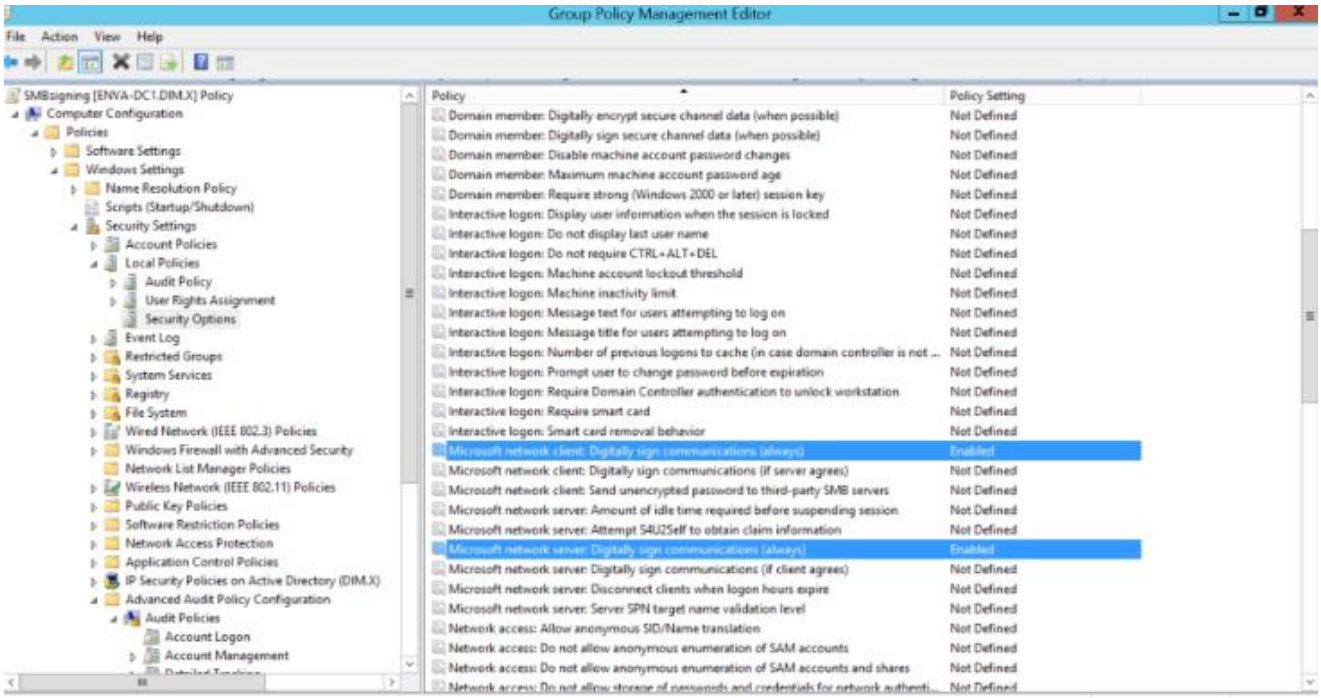
Для защиты от SMB Relay рекомендуется включить подпись SMB. Включение подписи SMB осуществляется путем редактирования значения реестра ОС. Однако настоятельно рекомендуется настраивать их с помощью групповых политик, а не изменять значения напрямую, поскольку групповые политики могут быть настроены по-разному и могут переопределять локальные изменения.

Важно отметить, что существует **три параметра** для подписи SMB:

- Enabled.
- Disabled.
- Required.

Рекомендуемый параметр - третий, заставляющий ОС взаимодействовать, используя только подписанные сообщения.

Включение подписи SMB можно выполнить с помощью объекта групповой политики. Чтобы включить принудительную подпись SMB, активируйте «Digital sign communication (always)» клиента и сервера:

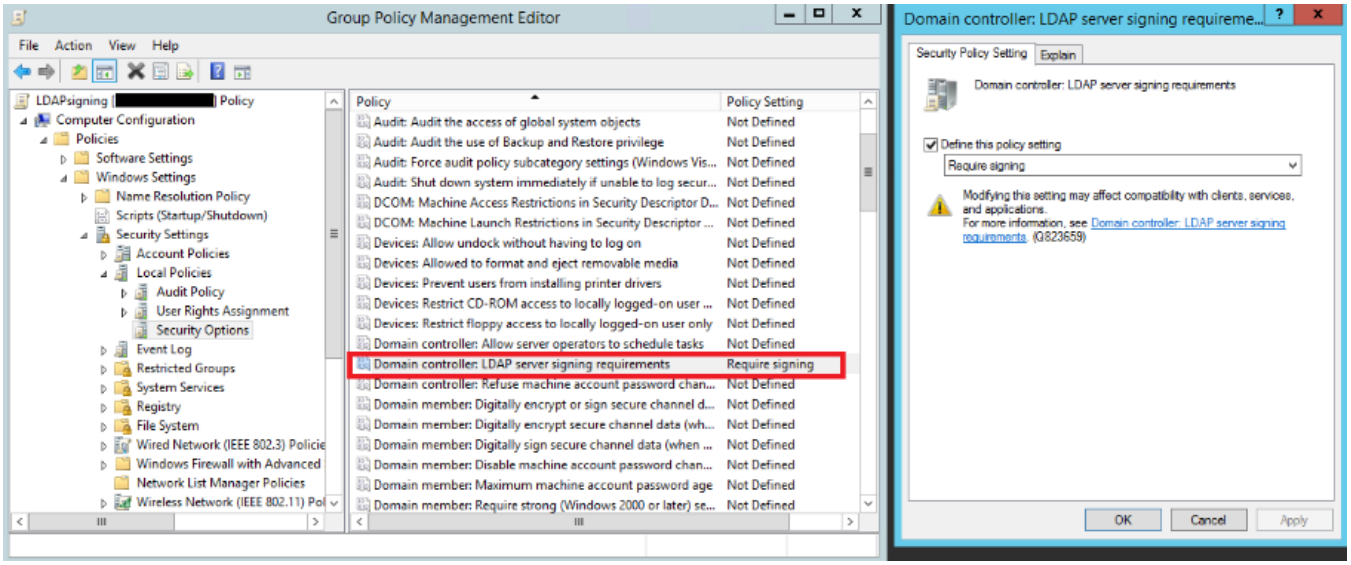


Рекомендации по защите от LDAPS Relay

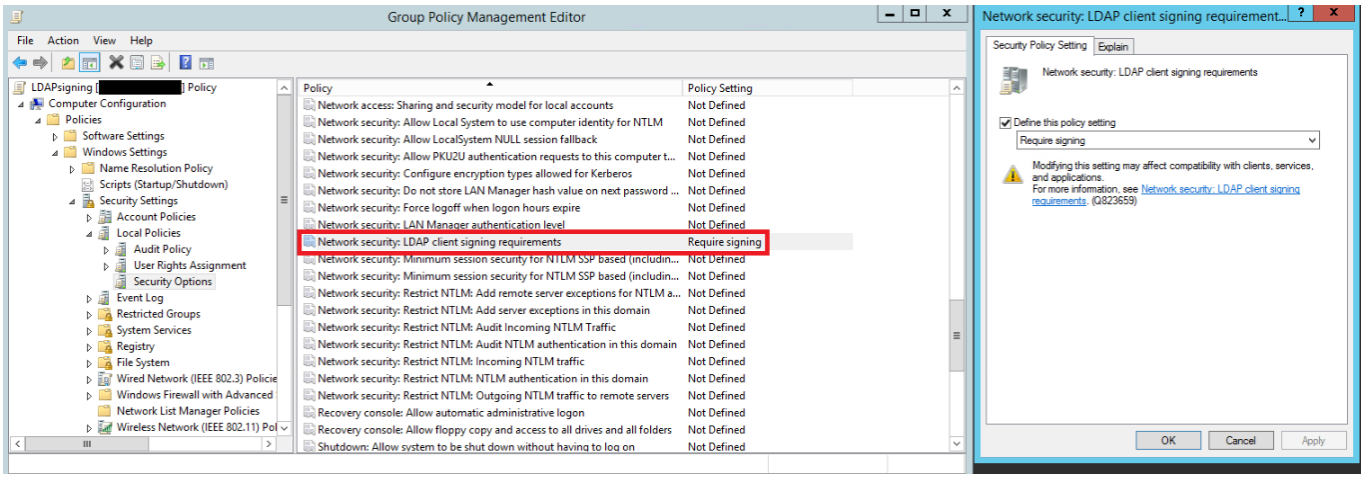
Неподписанный сетевой трафик подвержен атакам типа «человек по середине», когда злоумышленник перехватывает пакеты между сервером и клиентским устройством и изменяет их перед пересылкой на клиентское устройство. В случае сервера LDAP это означает, что злоумышленник может заставить клиентское устройство принимать решения на основе ложных записей из каталога LDAP. Уязвимость заключается в том, что, хотя подпись LDAP защищает как от Man-in-the-Middle (MitM), так и от пересылки учетных данных, LDAPS защищает от MitM (при определенных обстоятельствах), но не защищает от пересылки учетных данных вообще. Это позволяет злоумышленнику в сети использовать любой входящий сеанс Net-NTLM и выполнять операции LDAP от имени пользователя. В результате каждое соединение с машины в сети с администратором домена приведет к тому, что злоумышленник создаст учетную запись администратора домена и получит полный контроль над атакуемой сетью.

LDAP:

Определите объект групповой политики, который устанавливает Domain controller:» LDAP server signing requirements» в значение «Require signature» (расположение: «Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options»).



Клиенты, не поддерживающие подписывание LDAP, не смогут выполнять запросы LDAP к контроллерам домена. Чтобы включить подписывание LDAP на стороне клиентов, определите другой объект групповой политики, который устанавливает Network Security: «LDAP client signing requirements» в «Require signature»:



LDAPS:

Установите соответствующее обновление Windows для CVE-2017-8563 на всех компьютерах в домене: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8563. На клиентских компьютерах, на которых не установлено это обновление, могут возникнуть проблемы с совместимостью, и ранее работавшие запросы аутентификации LDAP через SSL / TLS могут больше не работать.

Настройте следующие параметры реестра HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/NTDS/Parameters:

DWORD: LdapEnforceChannelBinding

DWORD value: 2

«2» означает постоянное включение. Все клиенты должны предоставить информацию о привязке канала. Сервер всегда отклоняет запросы аутентификации от клиентов, которые не включены.