Содержание

Вопрос

Каково различие между NTLM и проверкой подлинности LDAP?

Среда

Cisco Web Security Appliance (WSA), все версии AsyncOS

Аутентификация с WSA может быть разломана на следующие возможности:

Клиент> WSA	WSA> Сервер проверки подлинности	Тип сервера проверки подлинности
Базовая аутентификация	Проверка подлинности LDAP	Сервер LDAP
Базовая аутентификация	Проверка подлинности LDAP	Сервер Active Directory с помощью LDAP
Базовая аутентификация	Базовая проверка подлинности NTLM	Сервер Active Directory (Основной NTLM)
Аутентификация NTLM	Аутентификация NTLMSSP	Сервер Active Directory (NTLMSSP)

Примечание: NTLMSSP обычно упоминается как NTLM.

Примечательное различие между Базовой проверкой подлинности и аутентификацией NTLM ниже.

Клиентский опыт

Основной

Клиенту будут всегда предлагать для учетных данных. После того, как учетные данные

были введены, браузеры будут, как правило, предлагать флажок для запоминания предоставленных учетных данных. Любое время браузер закрыт, клиент, вызовет снова или передаст ранее помнившие учетные данные снова.

Примечание: Основной NTLM использует Базовую проверку подлинности от клиента и таким образом будет иметь те же свойства.

NTLM (SSP)

- Клиент будет прозрачно используемая аутентификация его учетные данные начала сеанса Windows.
- Единственные случаи, в которых клиент вызовет для учетных данных, - то, если учетные данные Windows сначала откажут (то это произойдет, если в клиента войдут локально к компьютеру а не к домену, используемому для аутентификации), или если клиент не доверяет WSA.

Безопасность

Основной

Учетные данные передаются неуверенно с помощью открытого текста. Перехват простого пакета между клиентом и WSA покажет имя пользователя и пароль пользователя.

NTLM (SSP)

Учетные данные передаются надежно через трехэтапное установление связи (аутентификация стиля дайджеста). Паролем является NEVER, передаваемый через провод.

Процесс NTLM выглядит как таковым:

1. Клиент передает NTLM, Выполняют согласование о пакете. Это говорит WSA, что клиент намеревается сделать аутентификацию NTLM.
2. WSA передает строку проблемы NTLM клиенту.
3. Клиент использует алгоритм на основе его пароля для изменения проблемы и передает ответ на запрос к WSA.
4. AD сервер тогда проверяет, что клиент использует правильный пароль на основе того, модифицировало ли это строку проблемы соответственно.