На что аутентификация NTLM должна быть похожей на пакетном уровне?

Содержание

Вопрос:

На что аутентификация NTLM должна быть похожей на пакетном уровне?

ip.addr == 165.2.2.129.158 клиентов
ip.addr == 165.202.2.150 WSA>

Пакетный номер / Подробные данные:

#4 клиент отправляет запрос GET к прокси

#6 прокси передает 407 обратно. Это означает, что прокси не позволяет трафик из-за отсутствия правильной проверки подлинности. При рассмотрении Заголовков HTTP в этом ответе вы будете видеть, что аутентифицируется "Прокси-: NTLM". Это говорит клиенту, что приемлемый метод проверки подлинности является NTLM. Аналогично, если аутентифицируется заголовок "Прокси-: Основной" присутствовали, прокси будет говорить клиенту, что основные учетные данные приемлемы. Если оба заголовка будут присутствовать (распространенные), то клиент решит, какой метод проверки подлинности это будет использовать.

Одна вещь обратить внимание состоит в том, что заголовком аутентификации является "Прокси - аутентифицируются":. это вызвано тем, что соединение в перехвате использует явный прямой прокси. Если бы это было развертываниями режима прозрачного прокси, то код ответа был бы 401, вместо 407, и заголовками был бы "www - аутентифицируются": вместо "прокси - аутентифицируются":.

#8 FIN прокси этот TCP - сокет. Это корректно и обычно.

#15 На новом TCP - сокете клиент выполняет другой запрос GET. На этот раз заметьте, что GET содержит Заголовок HTTP "авторизация прокси":. это содержит закодированную строку, которая содержит подробные данные относительно Пользователя / Домен.

При расширении авторизации Прокси> NTLMSSP вы будете видеть декодируемую информацию, передаваемую в данных NTLM. В "Типе сообщения NTLM", вы заметите, что это - "NTLMSSP_NEGOTIATE". Это - первый шаг 3 способами квитирование NTLM.

#17 прокси отвечает еще 407. Другой "прокси - аутентифицирует" заголовок, присутствует. На этот раз содержание NTLM бросает вызов строке. При расширении его далее вы будете

видеть, что Тип сообщения NTLM является "NTLMSSP_CHALLENGE". Это - Действие второе 3 способами квитирование NTLM.

В аутентификации NTLM контроллер домена Windows передает строку проблемы клиенту. Клиент тогда применяет алгоритм к факторингу проблемы NTLM в пароле пользователей в процессе. Это позволяет контроллеру домена проверять, что клиент знает правильный пароль, никогда не передавая пароль через линию. Это намного более безопасно тогда основные учетные данные, в которых пароль передается в открытом тексте за всеми анализаторами для наблюдения.
#18 Клиент передает заключительный GET. Обратите внимание на то, что этот GET находится на ТОМ ЖЕ TCP - сокете как это, NTLM Выполняет согласование, и проблема NTLM произошла на. Это жизненно важно для процесса NTLM. Все квитирование должно произойти на ТОМ ЖЕ TCP - сокете, иначе аутентификация будет недопустима.

В этом запросе клиент передает модифицированную проблему NTLM (Ответ NTLM) к прокси. Это - заключительный шаг 3 способами квитирование NTLM.
#20 прокси передает Ответ HTTP обратно. Это означает, что прокси принял учетные данные и решил подать содержание.