**Лабораторная работа 1**

**Изучение протоколов сетевой аутентификации в сетях ОС Windows**

**Цель лабораторной работы**

1. Познакомиться с интерфейсом управления ролей *Windows Server*.
2. Познакомиться со структурой контроллера домена.
3. Изучить процесс аутентификации по протоколу *NTLMv2* и *Kerberos*.

**Используемое программное обеспечение**

Для выполнения лабораторной работы используются ОС *Windows Server 2012* и *Windows 7*.

**Порядок выполнения работы**

1. Подключиться к *Windows Server 2012 R2* и *Windows 7*. Информацию о параметрах и способе подключения, получить у преподавателя.

**Windows Server 2012 R2**

Логин – Администратор

Пароль – Student123

**Windows 7**

Логин – admin

Пароль – student

1. На *Windows Server* интерфейсе**Ethernet0** настроить параметры сети:

|  |  |
| --- | --- |
| IP адрес | 192.168.0.1 |
| Маска подсети | 255.255.255.0 |
| Шлюз | - |
| DNS | 127.0.0.1 |

1. На *Windows client* интерфейсе настроить параметры сети:

|  |  |
| --- | --- |
| IP адрес | 192.168.0.5 |
| Маска подсети | 255.255.255.0 |
| Шлюз | 192.168.0.1 |
| DNS | 192.168.0.1 |

1. Отключить брандмауэр (самостоятельно настроить) на обоих ПК.
2. На рабочем столе Windows Server создать папку «*Share»*.
3. Открыть эту папку для общего доступа пользователю «*Administrator*» (Используя Свойства → Доступ → Общий доступ).
4. Скачать по Wireshark 2.2.6 с сетевой папки, введя адрес в окне «Мой компьютер»:

**\\nas1.zss.local\p\ЗОС ИБ\Софт**

Логин: **zss\student**

Пароль: **student**

1. Запустить программу *Wireshark* на *Windows Server* с перехватом пакетов с аутентификации *NTLM* на интерфейсе *LAN*.

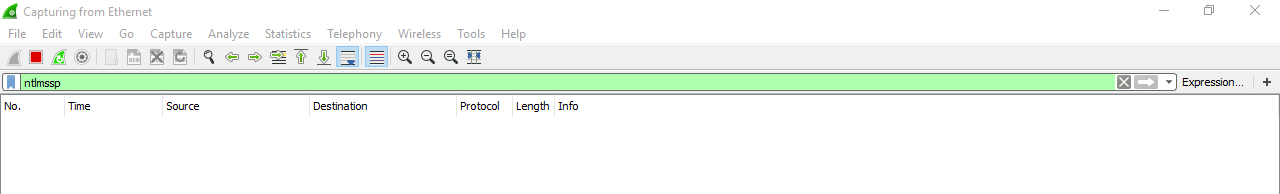


Рис. 1 Фильтрация по протоколу

1. С *Windows Client* получить доступ к сетевому ресурсу и перехватить пакеты аутентификации (пройти по адресу **\\192.168.1.1**).

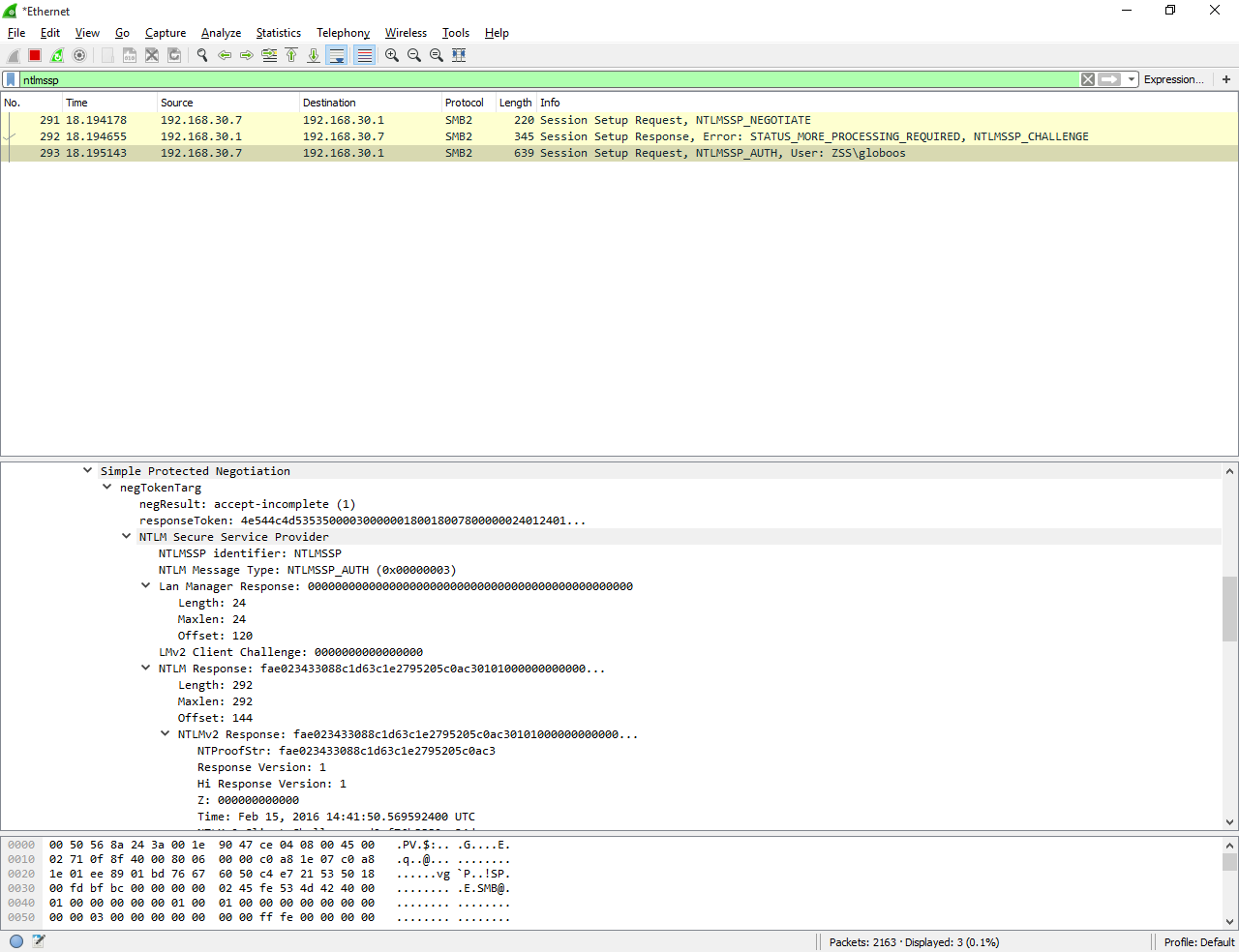


Рис. 2 Аутентификация NTLM в рамках протокола SMB

1. Изучить все информацию, по аутентификации вложенную в пакет. Найти NTLMv2 ответ (NTLMv2 Response). Отобразить содержание пакета с ответом в отчете.
2. Задать имя Windows Server (поле Computer name) – srvpod[номер бригады]. Например «srvpod2».
3. С помощью «Установка ролей», развернуть контролер домена «*domain.local*» с паролем администратора «*Student123*».
4. Выберете «Доменные службы Active Directory».
5. После установки, повысить уровень до контролера домена.
6. После полной установки и настройки перегрузить сервер.
7. Авторизоваться на сервере с новым паролем, запустить «*Wireshark*».
8. Настроить фильтр на *IP*-адрес клиента.

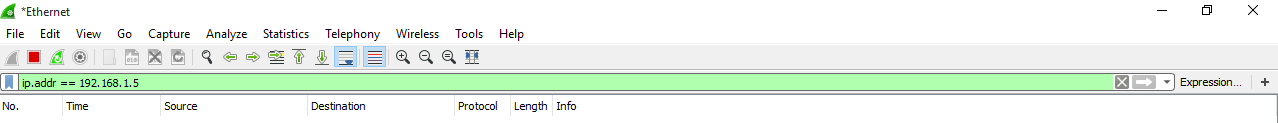


Рис.3 Фильтрация по IP-адресу

1. Ввести клиента в домен, изучить процедуру ввода клиента в домен на основе перехваченных пакетов.
2. Дождаться перезагрузки клиента и настроить фильтрацию по протоколу «*Kerberos*».
3. Просмотреть процесс ввода клиента в домен, с точки зрения сетвых пакетов.
4. Создать пользователя «*User*» с паролем «*Student123*» в «*Диспетчер ресурсов сервера →Средства → Пользователи и компьютеры Active Directory → <Имя домена> → Пользователи*».
5. Перехватить пакеты аутентификации клиента на сервере, при входе доменного пользователя на клиентском ПК (Аутентификация на client с логином «domain\User» и установленным паролем).
6. Изучить алгоритм авторизации клиента по средством протокола «*Kerberos*» (установить фильтр в *Wireshark* «*kerberos*»).
7. Найти пакеты, в которых передаются «TGT» и «TGS».  В отчете отобразить зашифрованные билеты (в сообщениях AS-REQ, AS-REP, TGS-REQ, TGS-REP).
8. Сохранить весь отчетный материал и завершить компьютеры в лабораторном стенде.

**Отчет должен содержать**

1. Титульный лист.
2. Текст задания.
3. Схема сети.
4. Скриншоты по выполненным действиям для пунктов 9,24.
5. Выводы.