ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ № 1

«Введение в безопасность сетей Windows»

«20» марта 2021 г.

Москва 2021 г.

СОДЕРЖАНИЕ

1. Необходимые условия для проведения лабораторной работы **3**
2. Подготовка виртуальных машин к проведению работы **4**
3. Проведение атаки **6**
4. Анализ дампа трафика **10**
   1. Установление соединения SMB 10
   2. Отправка Negotiate-пакета на аутентификацию NTL 10
   3. Отправка ответного Challenge-пакета 11
   4. Отправка запроса на анонимную аутентификацию 11
   5. Отправка «большого» пакета для переполнения буфера в сервисе SMB 12
   6. Отправка пакета с запросом доступа к шаре «ADMIN$» 13
   7. Отправка ответного пакета доступа к шаре «ADMIN$» 13
   8. Отправка пакета с запросом на запись в файл 14
   9. Отправка пакета с запросом на запись в файл содержимого исполняемого файла 14
   10. Отправка пакета на открытие и запуск службы 14
   11. Отправка пакета на удаление службы 15
   12. Отправка пакета на коммуникацию в рамках Meterpreter- сессии 15

5 Итоги проведения лабораторной работы **16**

1. Необходимые условия для проведения лабораторной работы

Для проведения работы нужно :

1. Наличие виртуальной машины Windows XP (или же цель, или атакуемая машина в дальнейшем);
2. Наличие виртуальной машины kali-linux (или злоумышленник, или атакующая машина в дальнейшем);
3. Наличие сетевого анализатора wireshark.

2 Подготовка виртуальных машин к дальнейшей с ними работы

Подготовка происходит следующим образом :

Переименовываю имя компьютера на виртуальной машине Windows XP на Morin-Denis (Рисунок 1).

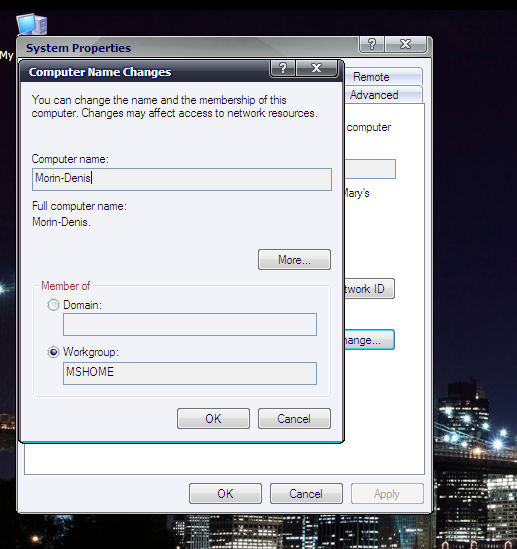


Рисунок 1 – имя компьютера Windows XP Morin-Denis

Фиксирую ip-адрес Windows XP (Рисунок 2).

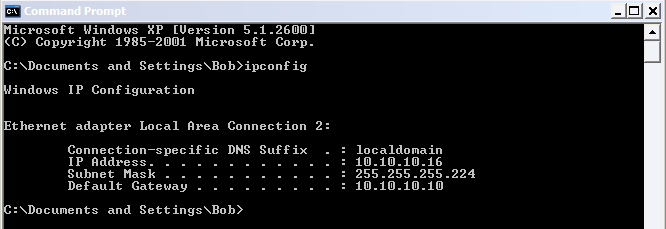


Рисунок 2 – ip-адрес Windows XP 10.10.10.16

Фиксирую ip-адрес kali-linux (Рисунок 3).

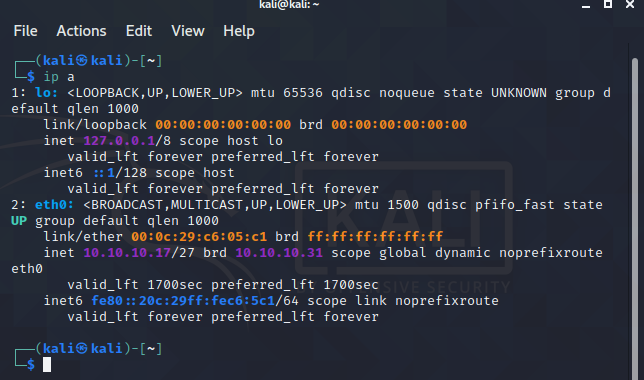


Рисунок 3 – ip-адрес kali-linux 10.10.10.16

Перед запуском Windows XP настраиваю фильтры на wireshark (Рисунок 4).

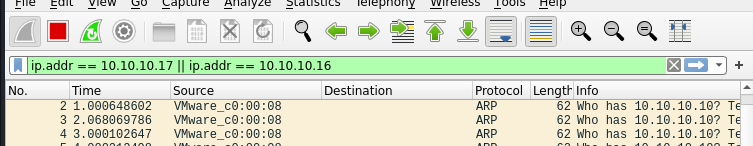


Рисунок 4 – фильтр на атакующую или атакуемую машину

3 Проведение атаки (с kali-linux на Windows XP)

Провожу атаку следующим образом :

Обновляю список пакетов (Рисунок 5).

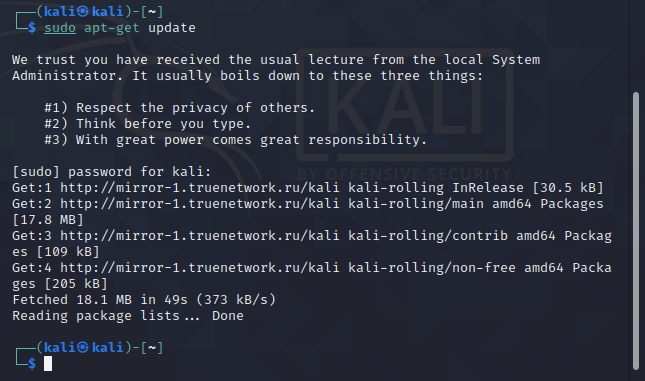


Рисунок 5 – синхронизация и обновление индексных файлов пакетов

Выполняю обновление пакетов, установленных в системе (Рисунок 6).

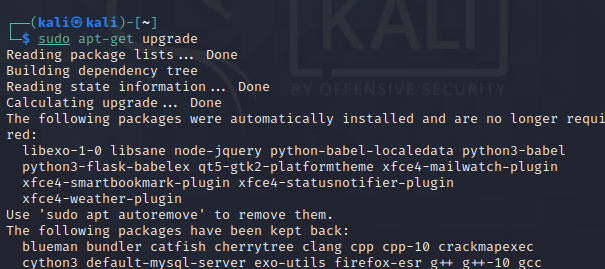


Рисунок 6 – обновление всего установленного на данный момент софта в системе

Запускаю Metasploit (Рисунок 7).

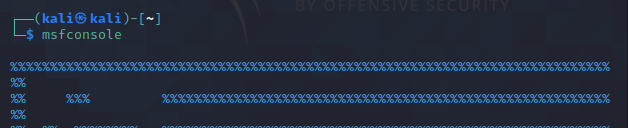


Рисунок 7 – запуск платформы для тестирования на проникновение

Устанавливаю exploit в активное состояние (Рисунок 8).

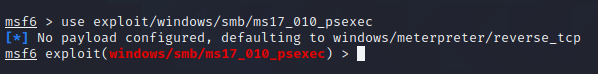


Рисунок 8 – запуск модуля «psexec»

Смотрю, какие доступные опции или параметры используются в exploit (Рисунок 9,10,11).

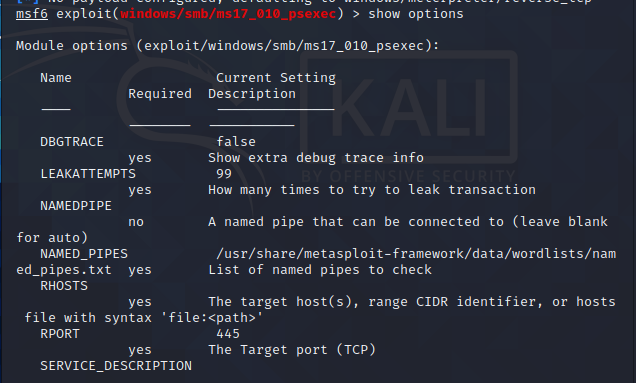


Рисунок 9 – просмотр текущих настроек

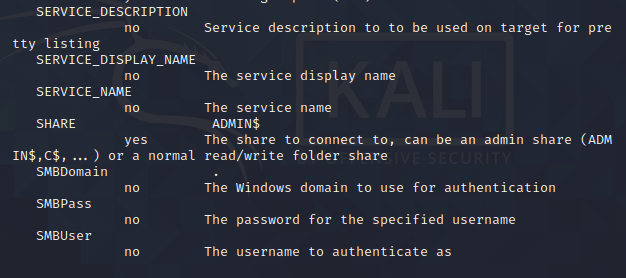


Рисунок 10 – просмотр текущих настроек (продолжение)

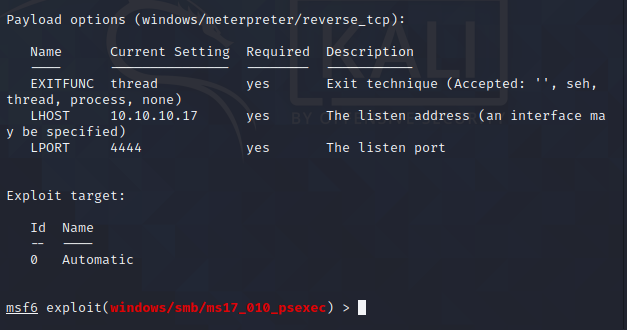


Рисунок 11 – просмотр текущих настроек (продолжение)

Указываю порт хоста Windows XP для его изучения (Рисунок 12).



Рисунок 12 – установка IP-адреса цели

Задаю адрес атакующего (Рисунок 13).



Рисунок 13 – IP-адрес машины

Эксплуатирую уязвимость (Рисунок 14).

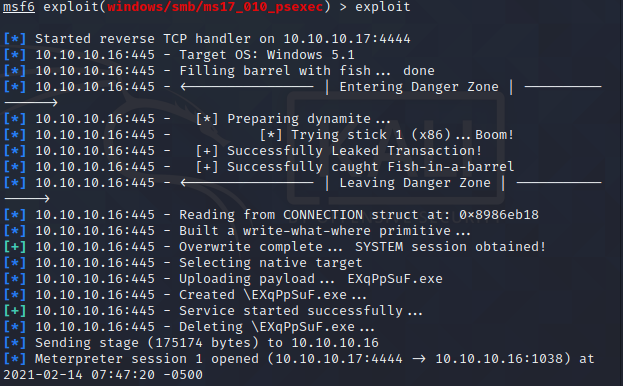


Рисунок 14 – захват контроля над системой

Проверяю доступ к хосту Windows XP (Рисунок 15).

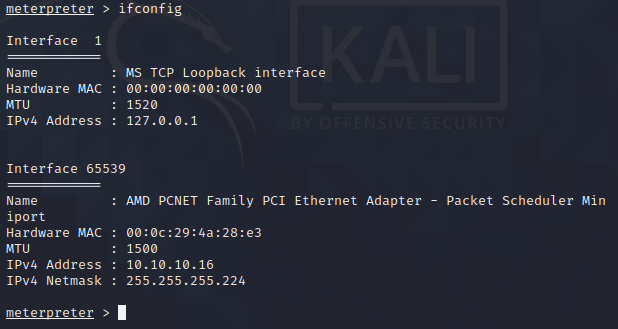


Рисунок 15 – получен доступ к Windows XP

Проверяю успешность эксплуатации на Windows XP (Рисунок 16).

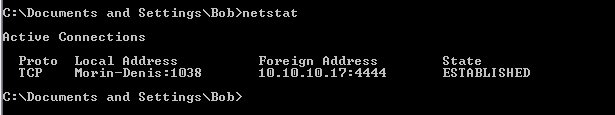


Рисунок 16 – существует доступ у Kali-linux (10.10.10.17) к Windows XP

1. Анализ дампа трафика
   1. Установление соединения SMB злоумышленником (Рисунок 1).

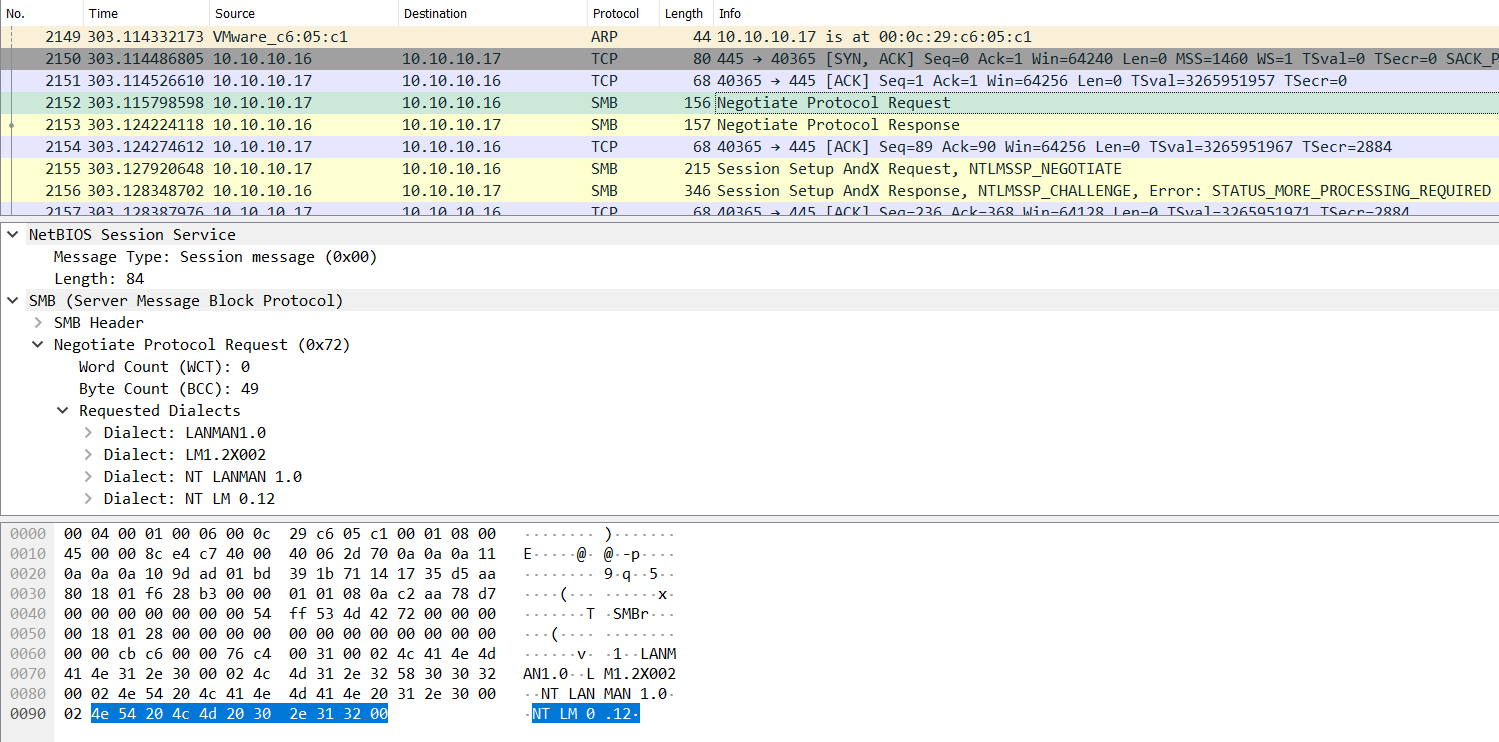


Рисунок 1 – отправка запроса на установление соединения

* 1. Злоумышленник отправляет Negotiate-пакет на аутентификацию NTLM (Рисунок 2).

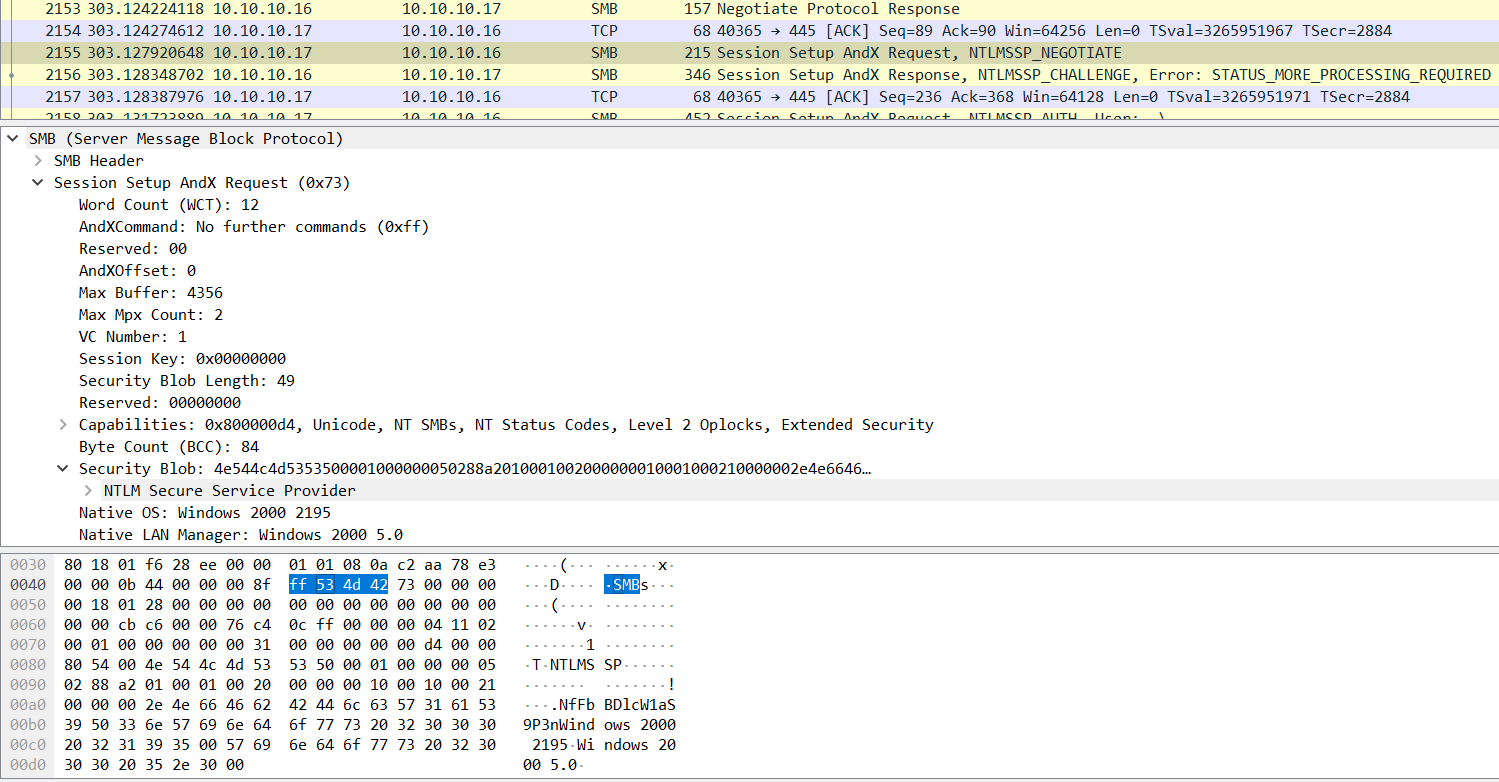


Рисунок 2 – запрос на аутентификацию NTLM

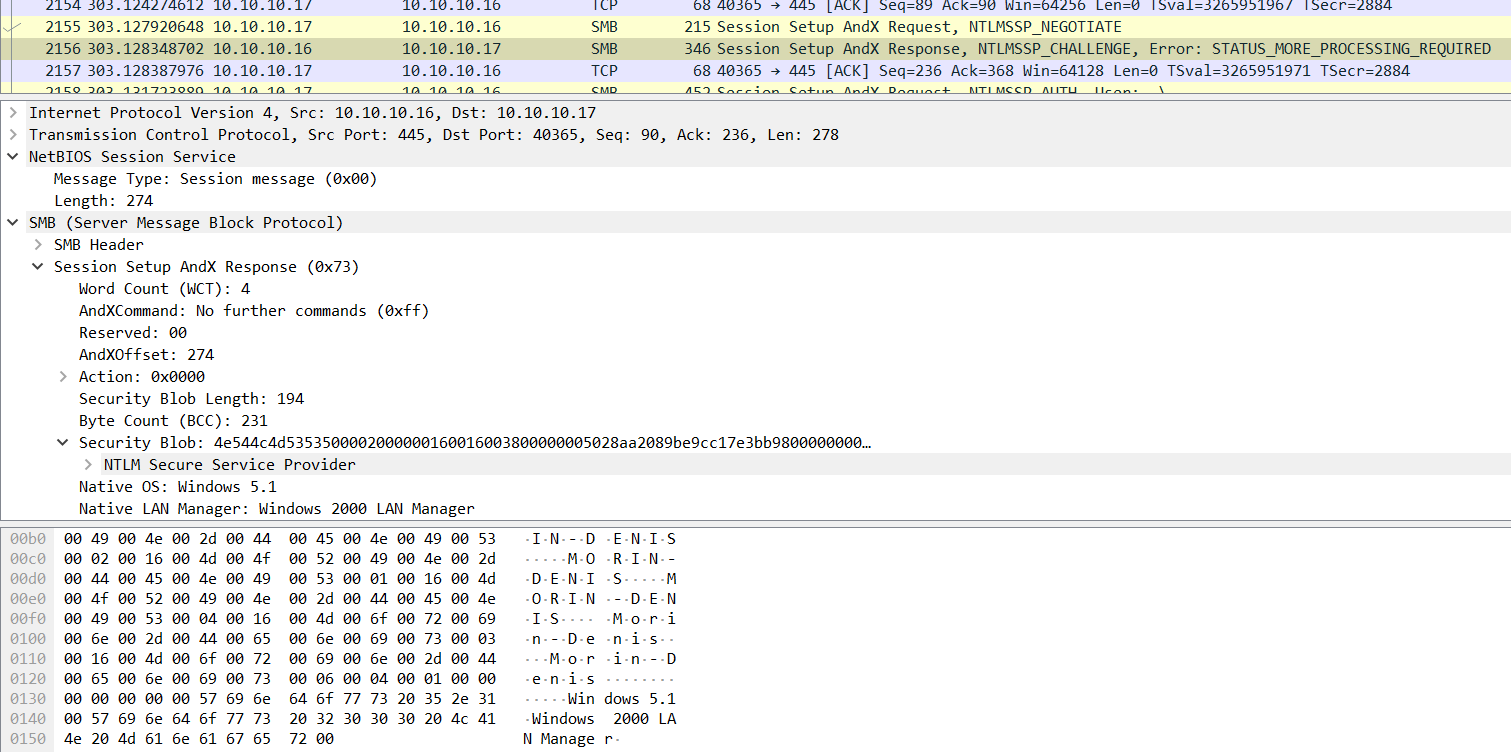
* 1. Windows XP отправляет ответный Challenge-пакет (Рисунок 3).

Рисунок 3 – отправка Challenge-пакета

* 1. Kali-linux пытается получить доступ к Windows XP (Рисунок 4,5).

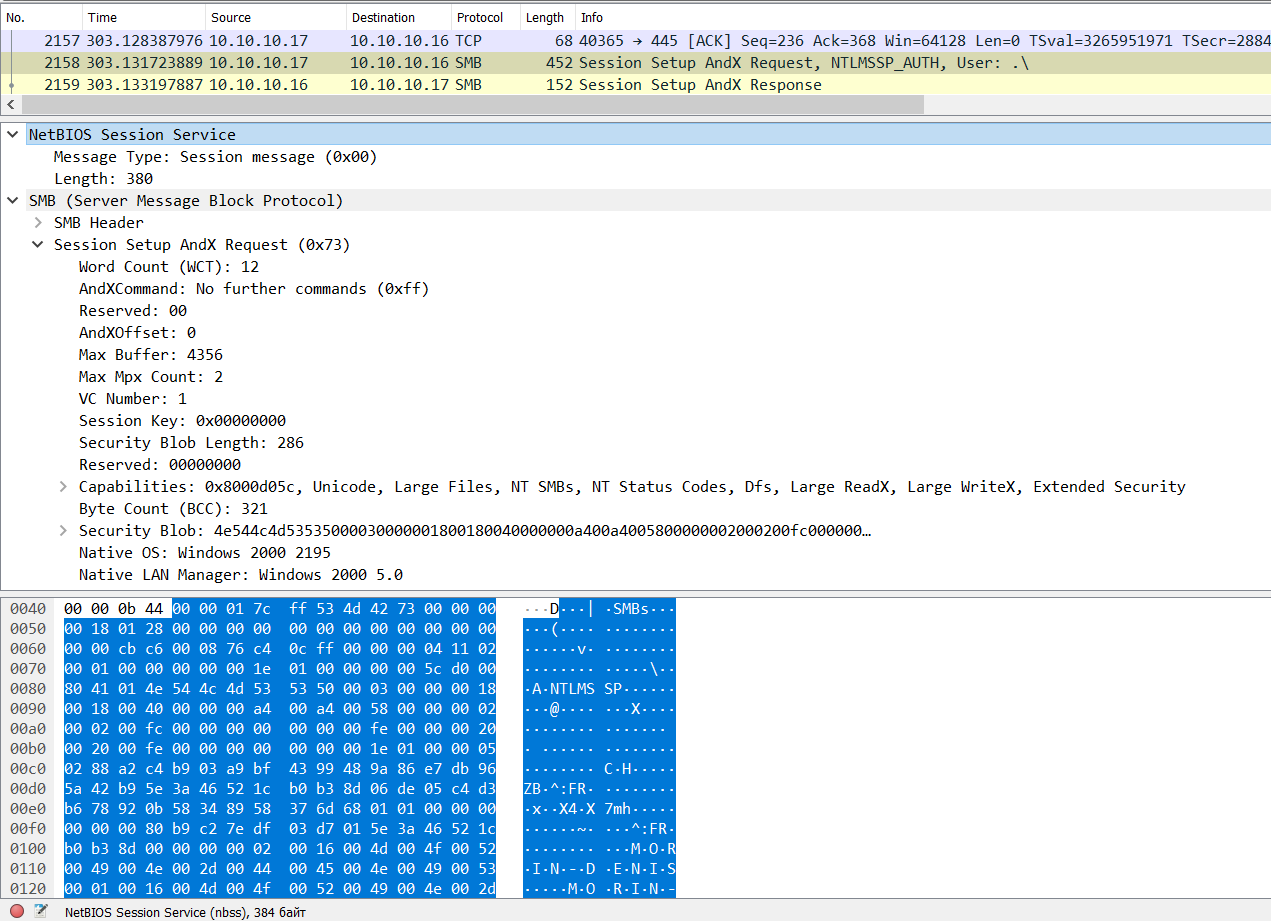


Рисунок 4 – запрос на анонимную аутентификацию

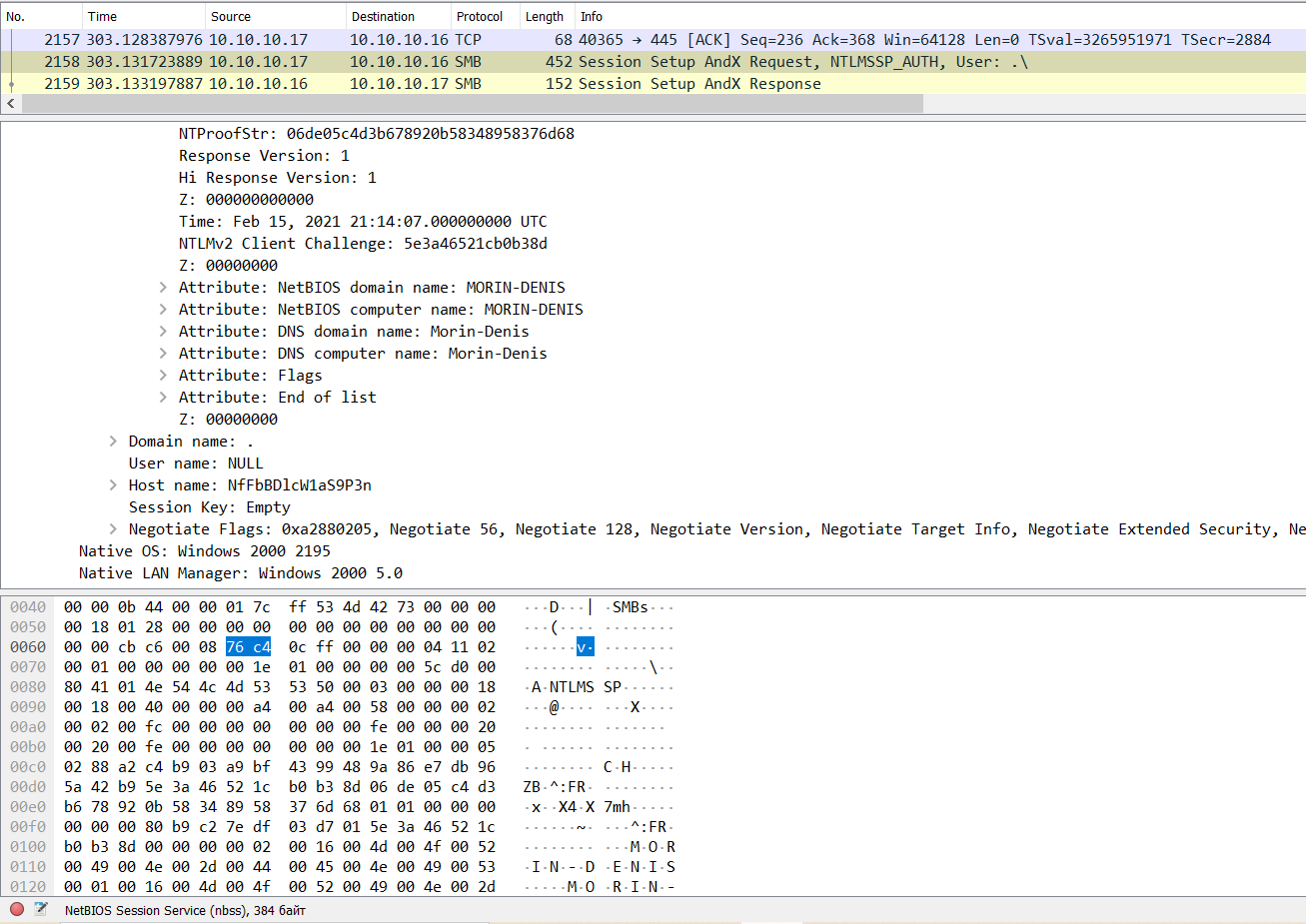


Рисунок 5 – запрос на анонимную аутентификацию (продолжение)

* 1. Злоумышленник отправляет «большие» пакеты для переполнения буфера (Рисунок 6).

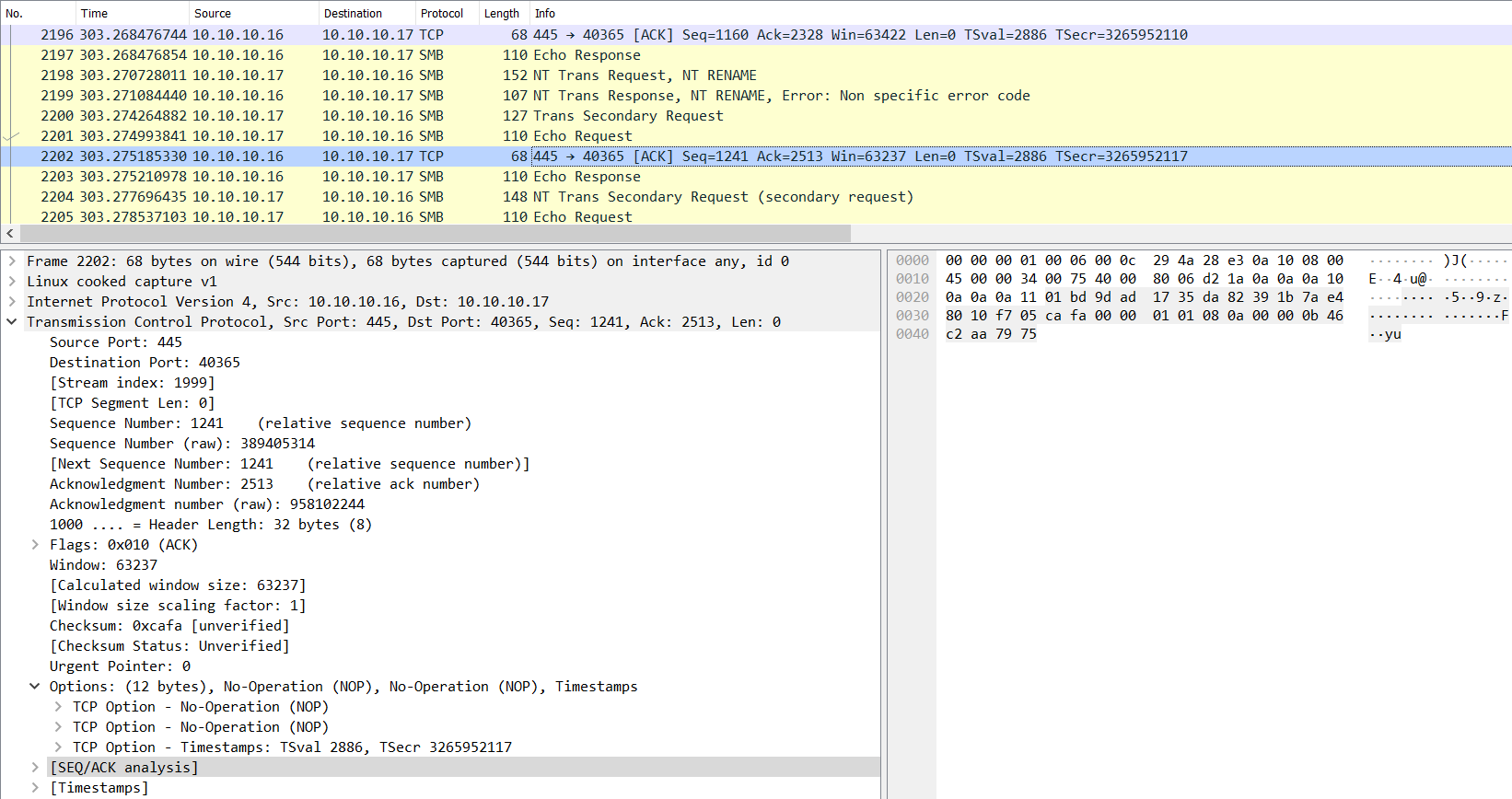
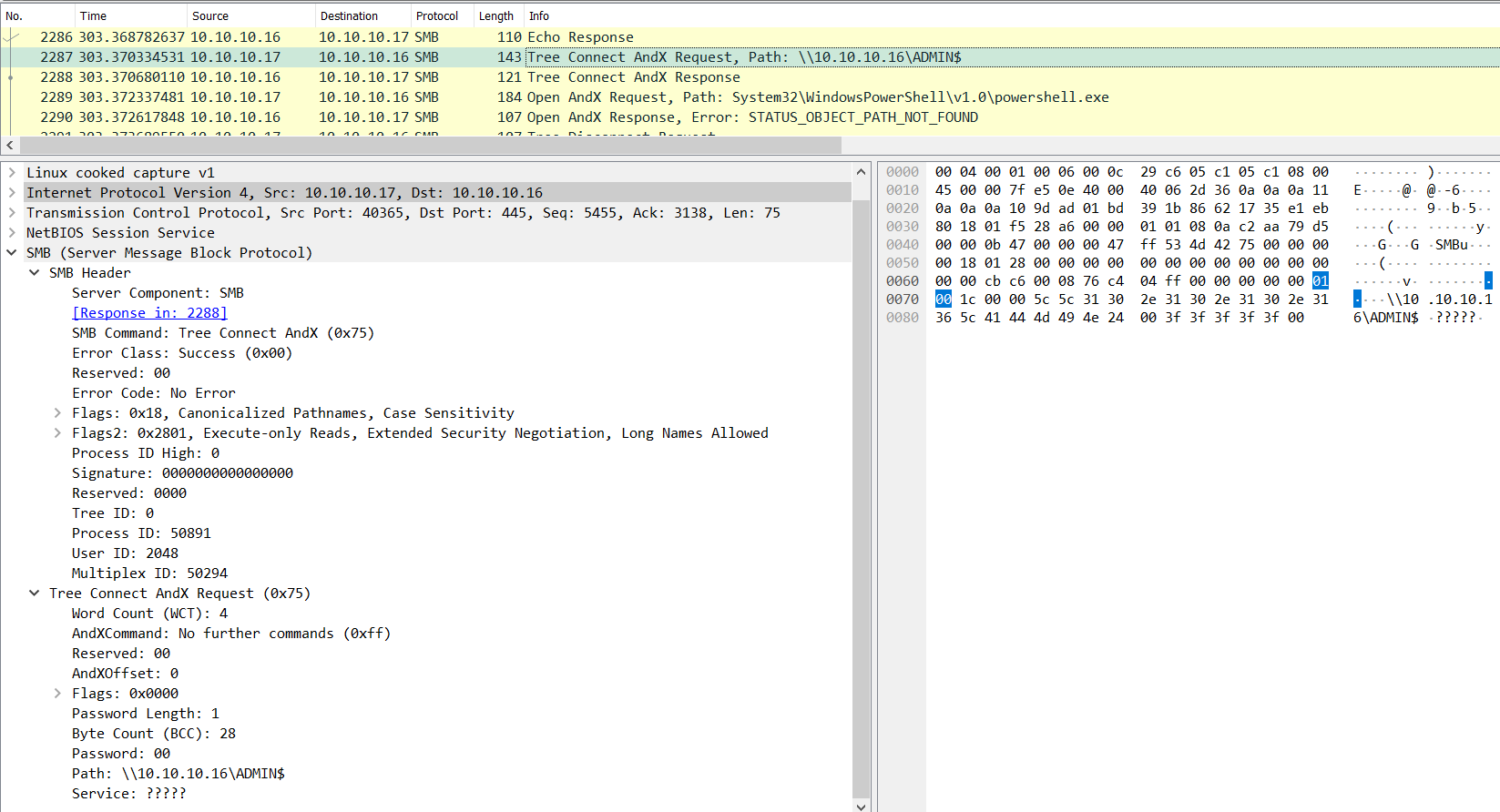


Рисунок 6 – отправка «большого» пакета

* 1. Злоумышленник смог подключиться к «ADMIN$» (Рисунок 7).

 Рисунок 7 – отправка пакета с запросом доступа к «ADMIN$»

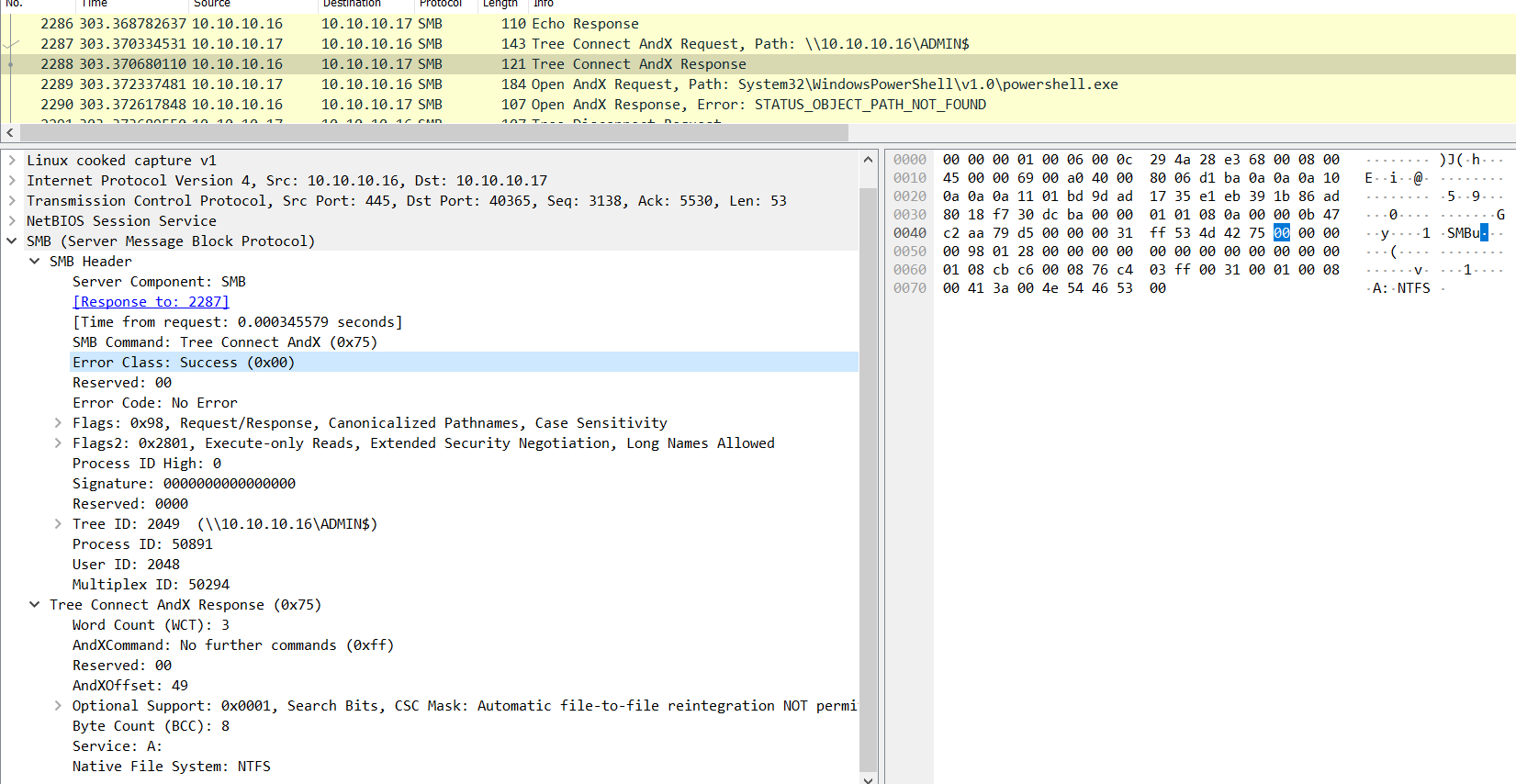
* 1. Windows XP отвечает на запрос к доступу «ADMIN$» (Рисунок 8).

Рисунок 8 – отправка ответного пакета доступа к шаре «ADMIN$» :

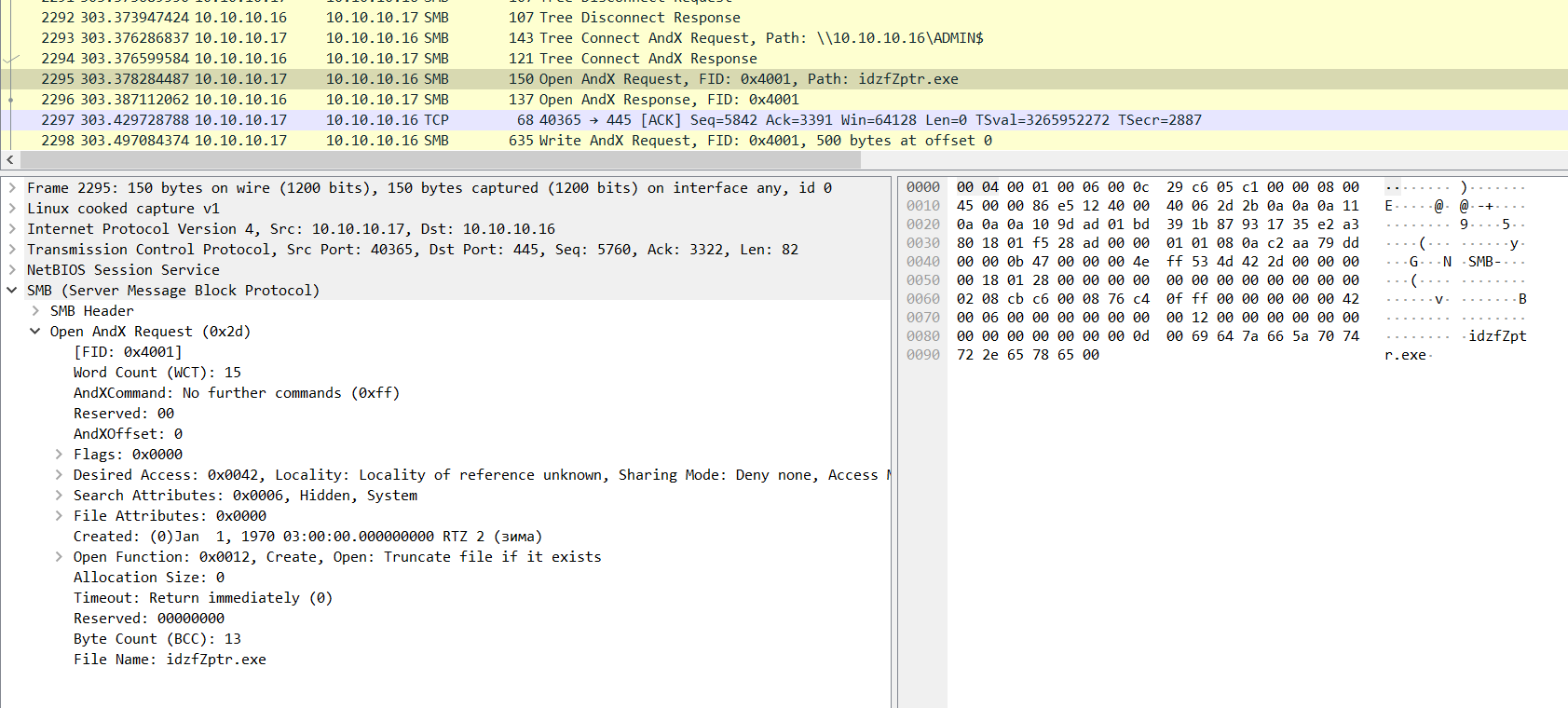
* 1. Kali-linux переподключается к Windows XP с идентификатором сессии 0х4001; ранее 0х4000 (Рисунок 9).

Рисунок 9 – отправка пакета с запросом на запись в файл idzfZptr.exe

* 1. При запросе на запись файла, злоумышленник посылает исполнительный файл (Рисунок 10).

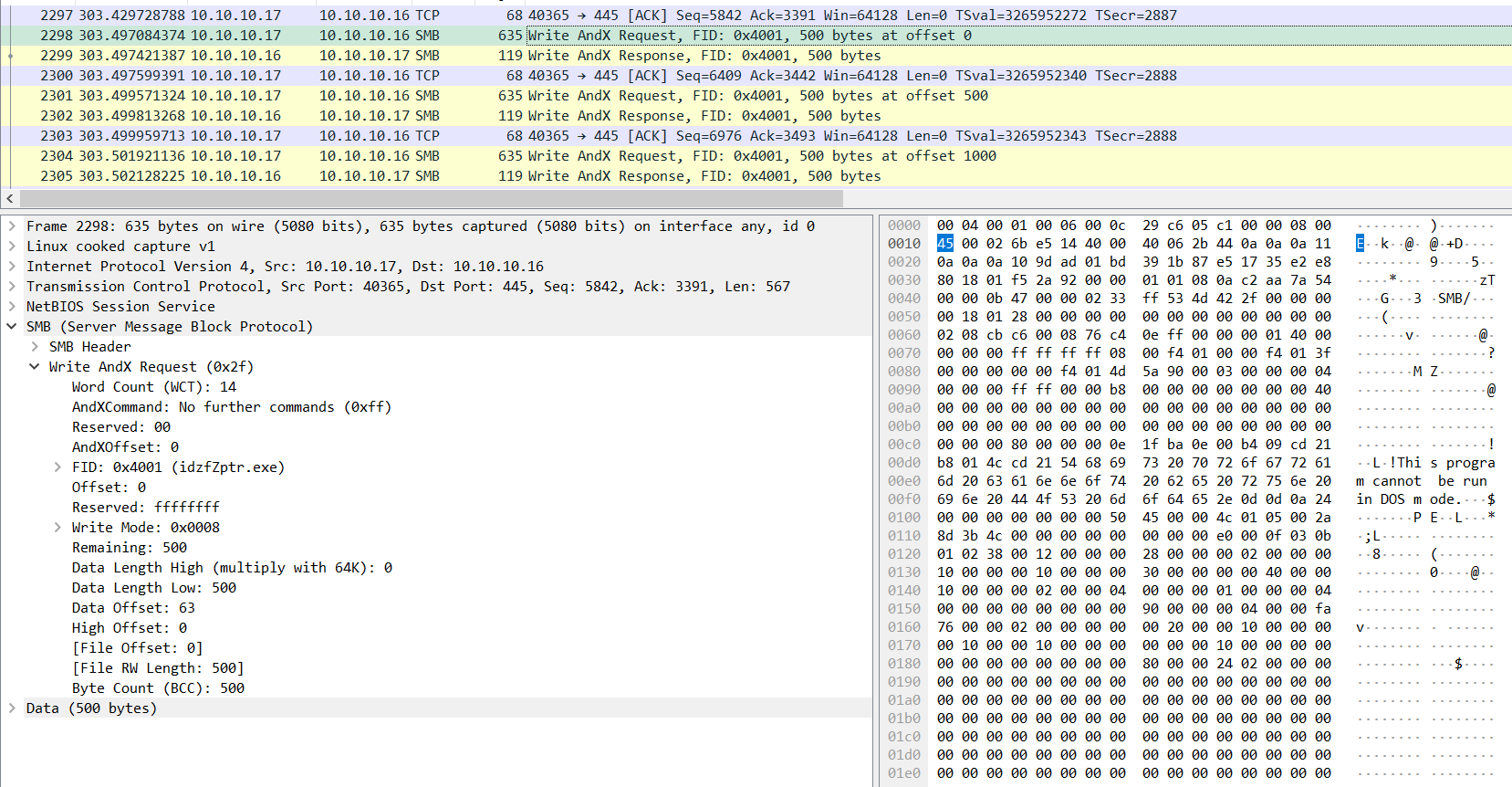


Рисунок 10 – запись в файл содержимого исполняемого файла

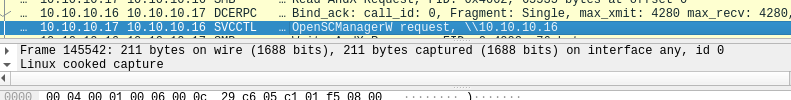
* 1. Kali-linux посылает запрос на доступ к OpenSCManagerW, благодаря этой функции злоумышленник сможет удаленно запускать / удалять службы (Рисунок 11).

Рисунок 11 – отправка пакета на открытие и запуск службы

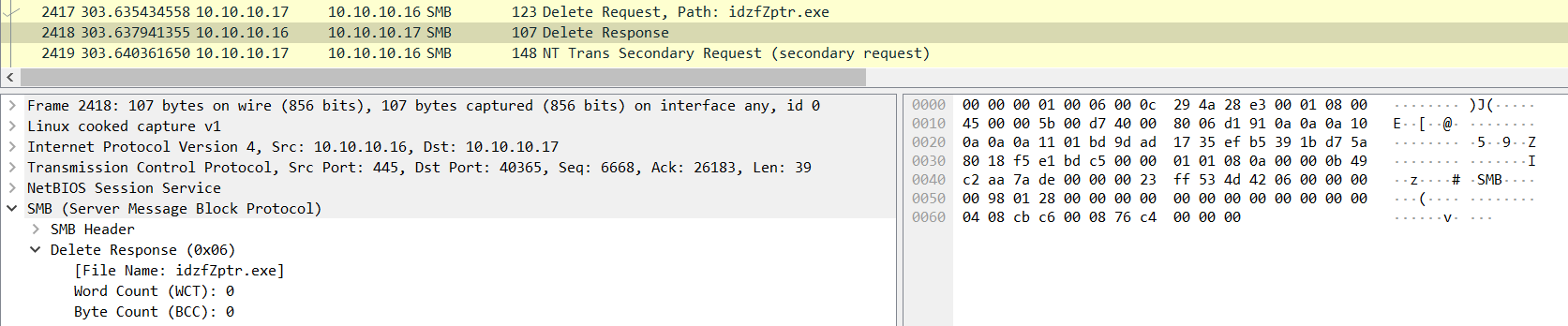
* 1. Злоумышленник подчищает свои следы атаки (Рисунок 12).

Рисунок 12 – отправка пакета на удаление службы для очистки следов атаки

* 1. Сессия с Meterpreter установлена. Для коммуникации с полезной нагрузкой Meterpreter атакующей машиной используется порт 4444 (Рисунок 13).

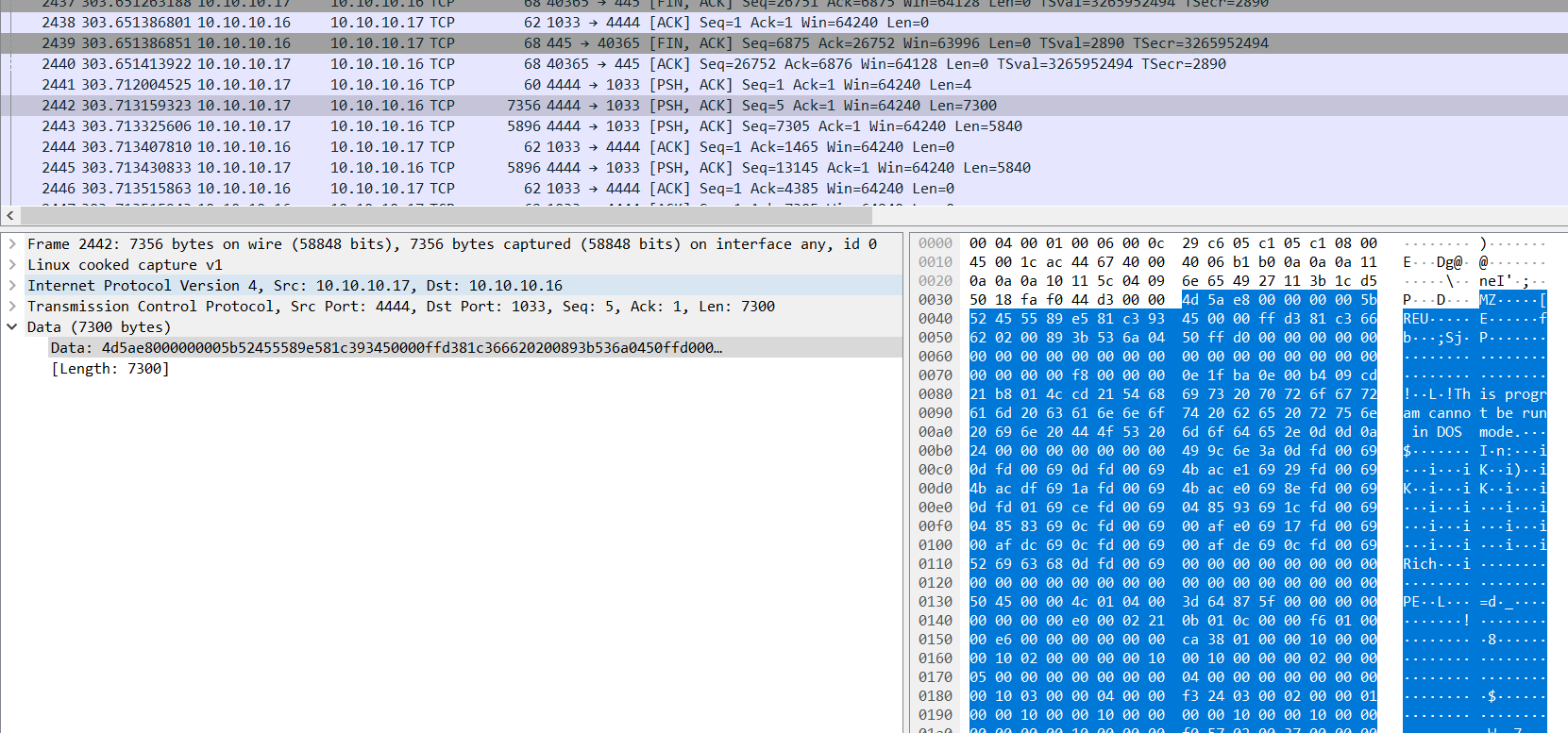


Рисунок 13 – отправка пакета на коммуникацию в рамках Meterpreter-сессии

1. Итоги проведения лабораторной работы
2. Основываясь на том, что злоумышленник успешно провёл свою атаку, можно сделать вывод о том, как плохо была защищена виртуальная машина Windows XP. Атакуемой машине следует улучшить свою защиту должным образом.
3. Проделав данную работу, для себя я узнал, как работать с платформой для тестирования на проникновение Metasploit, а также анализировать этапы атаки, реализованных с её помощью (через wireshark).