Протокол Kerberos

Основы информационной безопасности

Ищенко Ирина

3 мая 2024

Российский университет дружбы народов имени Патриса Лумумба, Москва, Россия

Докладчик

- Ищенко Ирина Олеговна
- НПИбд-02-22
- Студ. билет: 1132226529

Рис. 1: Протокол Kerberos

Введение

Протокол Kerberos - криптографический протокол, использующий механизм взаимной аутентификации. Протокол работает на основе тикетов, позволяя узлам обмениваться данными по незащищенной сети для подтверждения своей личности. Kerberos предназначен для обеспечения безопасности и аутентификации.

Идентификация - присвоение пользователям идентификаторов (уникальных имен или меток) под которыми система “знает” пользователя.

Аутентификация - установление подлинности - проверка принадлежности пользователю предъявленного им идентификатора.

Реализация Kerberos по архитектуре “клиент-сервер”

Клиентская часть устанавливается на все компьютеры защищаемой сети, кроме тех, на которые устанавливаются компоненты сервера Kerberos.

Серверная часть Kerberos называется центром распределения ключей (англ. Key Distribution Center, сокр. KDC) и состоит из двух компонент:

- сервер аутентификации (англ. Authentication Server, сокр. AS);
- сервер выдачи разрешений (англ. Ticket Granting Server, сокр. TGS).

Основные этапы

1. Вход пользователя / клиента
2. Аутентификация клиента / AS
3. Аутентификация клиента / службы
4. Клиент / запрос службы

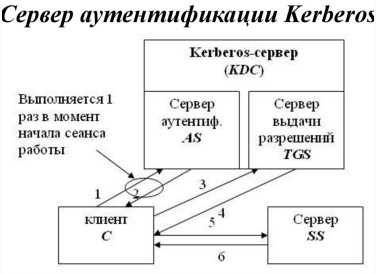
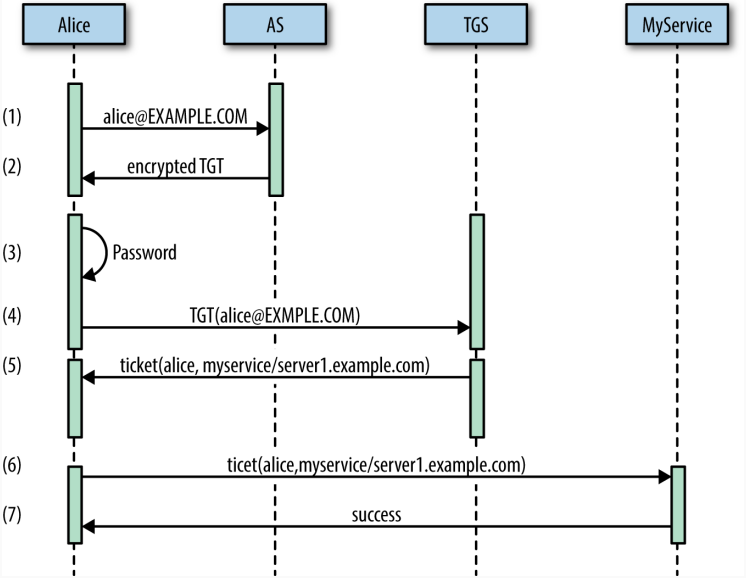


Рис. 2: Протокол Kerberos

Пошагово


Alice
AS
TGS
MyService
(1)
alice@EXAMPLE.COM
(2)
encrypted TGT
(3)
Password
(4)
TGT(alice@EXMPLE.COM)
(5)
ticket(alice, myservice/server1.example.com)
(6)
ticet(alice,myservice/server1.example.com)
(7)
success

AS-REQ

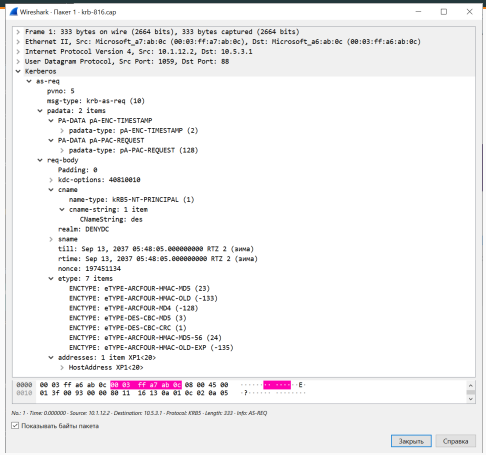


Рис. 4: Пакет 1

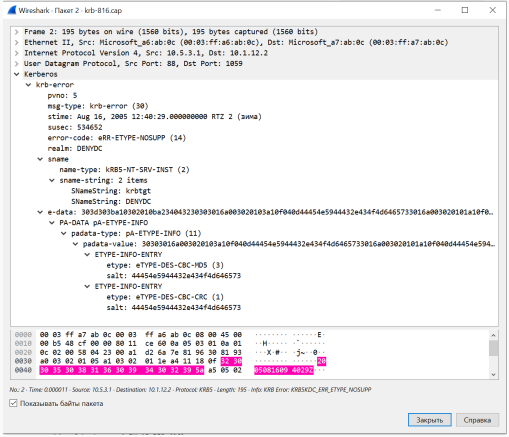


Рис. 5: Пакет 2

AS-REQ AS-REP

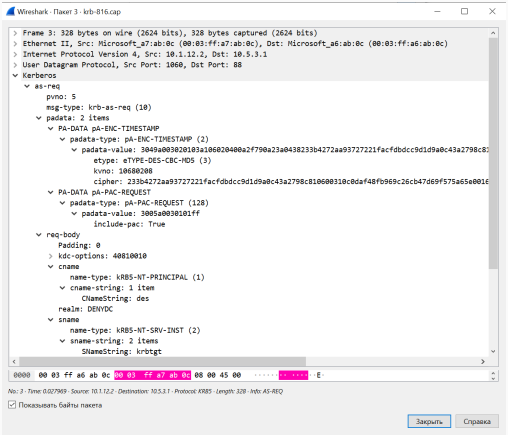


Рис. 6: Пакет 3

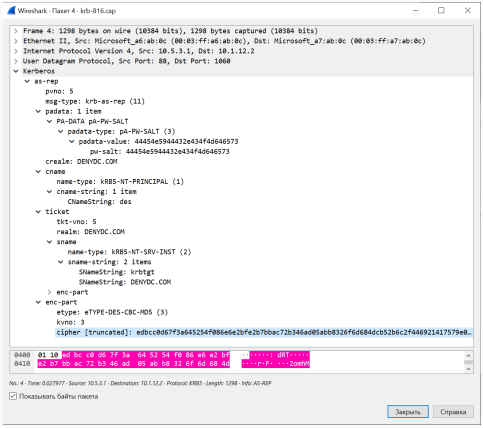


Рис. 7: Пакет 4

TGS-REQ TGS-REP

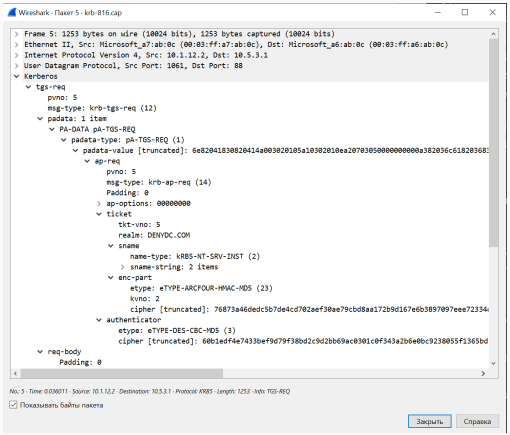


Рис. 8: Пакет 5

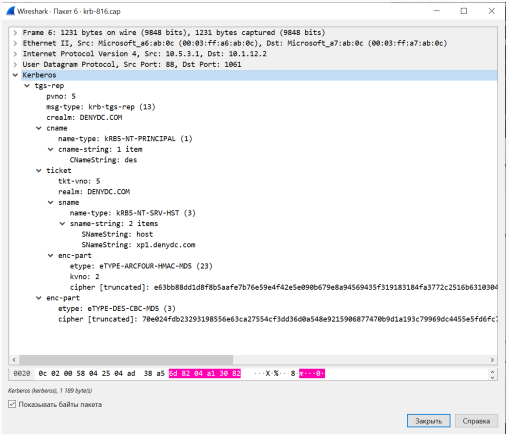


Рис. 9: Пакет 6

Заключение

Преимуществами протокола Kerberos являются высокая степень безопасности, возможность использования единого ключа шифрования для всех пользователей и серверов, а также простота реализации. Поддержка Kerberos встроена во все основные компьютерные операционные системы, включая Microsoft Windows, Apple macOS, FreeBSD и Linux. Срок действия билетов в Kerberos ограничен. Если билет будет украден, его будет сложно использовать повторно из-за необходимости строгой аутентификации. Пароли никогда не передаются по сети. Обе стороны (клиент и сервер) взаимно аутентифицируют друг друга с помощью протокола.

Однако у него есть и некоторые недостатки, такие как необходимость наличия централизованного сервера Kerberos и возможность атаки со стороны злоумышленников.

Спасибо за внимание