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

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

Сервер аутентификации Kerberos

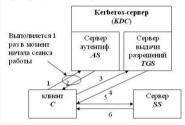
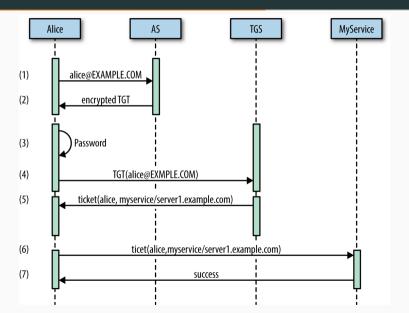
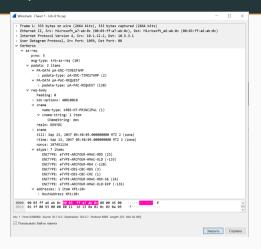


Рис. 2: Протокол Kerberos

Пошагово



AS-REQ



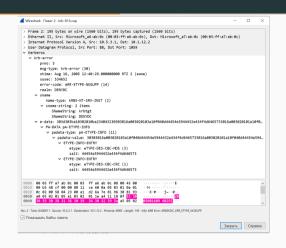
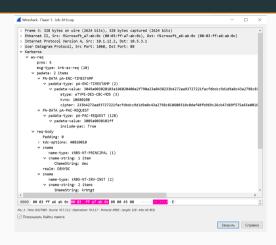


Рис. 4: Пакет 1

Рис. 5: Пакет 2

AS-REQ AS-REP



> Frame 4: 1298 hutes on wine (18384 hits) 1298 hutes centured (18384 hits) * Internet Protocol Version 4 Sec. 18 5 3 1 Det: 18 1 12 2 > User Datagram Protocol, Src Port: 88, Dst Port: 1868 w Kerhenne w as-cen nunn: 5 msg-type: krb-as-rep (11) v padata: 1 item ✓ PA-DATA pA-PW-SALT v padata-type: pA-PW-SALT (3) padata-value: 44454e5944432e434f4d646573 pu-salt: 44454e5944432e434f44646573 crealm: DENYDC.COM v cnave name-type: kRB5-NT-PRINCIPAL (1) v cname-string: 1 item CNameString: des v ticket tkt-vno: 5 realm: DENVDC.COM v sname name-type: kRBS-NT-SRV-INST (2) v sname-string: 2 items SNameString: krhtgt SNameString: DENVDC.COM > enc-part w enconant etype: eTYPE-DES-CBC-MD5 (3) kynn: 3 rinher [fruncated]: edhrr@d67f3a645254f@85e5e2hfe2h7hhar72h3d6ad@5ahh8326f6d68ddrh52h6r2f4d6Q21d1757ge8 0400 01 10 ed bc c0 d6 7f 3a 64 52 54 f0 86 e6 e2 b 8418 e2 b7 bb ac 72 b3 46 ad 85 ab b8 32 6f 6d 68 4d No.: 4 - Timer 0.027977 - Source: NO.S.2.1 - Destination: 10.1.12.2 - Protocol: KNRS - Length: 1298 - Info: AS-REP Помазывать байты памета Samura Consera

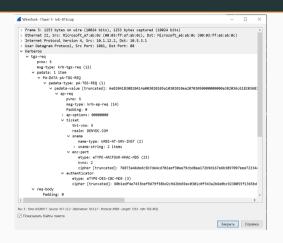
■ Wreshark - Flavor 4 - John 816 can

Рис. 6: Пакет 3

Рис. 7: Пакет 4

пх

TGS-REQ TGS-REP



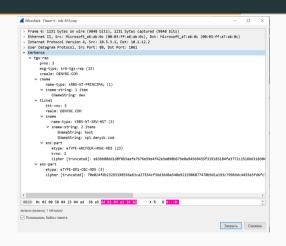


Рис. 8: Пакет 5

Рис. 9: Пакет 6

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