"KERBEROS V5 Y DIAMETER"

Trabajo Preparatorio N°6

Laboratorio de Seguridad en Redes

Melanny Dávila
Ingeniería en Telecomunicaciones
Facultad de Eléctrica y Eléctronica
Quito, Ecuador
melanny.davila@epn.edu.ec

Alejandra Silva
Ingeniería en Telecomunicaciones
Facultad de Eléctrica y Eléctronica
Quito, Ecuador
alejandra.silva@epn.edu.ec

***Abstract*—En el siguiente documento se presenta el sustento teórico acerca del protocolo Kerberos y su funcionamiento con el fin de implementar un ataque de autenticación de usuarios. Asimismo, se busca comprender el funcionamiento de Diameter.**

***Index Terms*—Kerberos, Diameter, autenticación, protocolo, contraseña**

I. Introducción

Kerberos es un protocolo de autenticación, pero no de autorización. Esto quiere decir que el protocolo se encarga de identificar a cada usuario, a través de una contraseña solo conocida por este, pero no determina a qué recursos o servicios puede acceder o no dicho usuario. Sus diseñadores se concentraron primeramente en un modelo de cliente-servidor, y brinda autenticación mutua: tanto cliente como servidor verifican la identidad uno del otro; se basa en criptografía de clave simétrica y requiere un tercero de confianza [1].

II. Objetivos

- Configurar e implementar el servicio de autenticación centralizada con base en el protocolo Kerberos.
- Configurar un servicio de red para que la autenticación del usuario se implemente utilizando el protocolo Kerberos.
- Configurar una entidad cliente para que se autentique mediante el protocolo Kerberos.
- Entender el funcionamiento de Diameter

III. Cuestionario

A. Revisar el marco teórico para la realización de la práctica.

B. Enumere y describa los ataques de autenticación a Kerberos. (máximo una carilla)

- **Overpass The Hash/Pass The Key (PTK):** Ataque que utiliza el hash del usuario para conseguir suplantar al mismo. Si un atacante consigue obtener el hash de un usuario podría suplantar a este frente al KDC, y acceder a los servicios del dominio disponibles para dicho usuario. Los hashes de usuario se pueden extraer de los ficheros SAM de las estaciones de trabajo, del fichero NTDS.DIT de los DC, o de la memoria del proceso lsass donde también es posible obtener las contraseñas en texto claro [1].
- **ASRERoast:** Busca el crackeo offline de las credenciales. Cuando un usuario está configurado con el atributo DONT_REQ_PREAUTH, no necesita preautenticación, con lo que es posible construir un mensaje KRB_AS_REQ sin conocer las credenciales del mismo. Una vez construído y enviado, el KDC responderá con un mensaje KRB_AS_REP que contiene datos cifrados con el hash de este usuario, pudiendo ser utilizados para el crackeo offline.
- **Pass The Ticket (PTT):** Se trata de obtener un ticket de usuario y utilizarlo para ganar acceso a los recursos para los que el usuario tenga permisos. Además del ticket, es necesario conseguir también la clave de sesión respectiva, para poder usar este en las comunicaciones con el servicio. Se pueden obtener los tickets mediante un ataque de Man-In-The-Middle, ya que estos viajan sobre UDP o TCP. No obstante, mediante este técnica no se consigue acceso a la clave de sesión [2].
- **Golden Ticket:** Busca construir un TGT, para lo cual se necesita la clave del krbtgt. Por tanto si se obtiene el hash NTLM de la cuenta krbtgt, es posible construir un TGT. Dicho TGT puede contar con la caducidad y permisos que se desee, consiguiendo incluso privilegios de administrador de dominio.
  El ticket continuará siendo válido aunque el usuario incluido cambie su contraseña. El TGT solo podrá ser invalidado si expira o cambia la contraseña de la cuenta krbtgt.
- **Silver Ticket:** Es similar a Golden Ticket, pero en este caso se construye un TGS y lo que se requiere es la clave del servicio al que se quiere acceder. Esta clave se deriva del hash NTLM de la cuenta propietaria del servicio. Esta técnica no funcionará si el servicio verifica el PAC, ya que al no conocer la clave de krbtgt, no es posible firmarlo correctamente.
- **Kerberoasting:** Trata de usar los TGS para realizar cracking de las contraseñas de los usuarios offline. Se debe tener en cuenta que con cualquier usuario de dominio es posible obtener un TGS para cualquier servicio,

debido a que Kerberos no se encarga de la autorización [1].

C. Consultar los detalles del proceso de autenticación mediante Kerberos, incluyendo particularmente los mensajes que intercambian el cliente, el KDC y el servidor de aplicación. (máximo una carilla)

Para el análisis del proceso de autenticación se parte de que el usuario no tiene ningún ticket.

1) El usuario solicita un Ticket Granting Ticket (TGT) del servidor de autenticación (AS), por lo que envía un *KRB_AS_REQ*, donde, entre otros, se pueden encontrar los siguientes campos en el mensaje:
   - Un timestamp cifrado con la clave del cliente, para autenticar al usuario y prevenir ataques de replay.
   - El nombre del usuario que se está autenticando.
   - El SPN del servicio asociado a la cuenta krbtgt.
   - Un nonce generado por el usuario
2) En cuanto este mensaje le llega al KDC se verifica la identidad del usuario descifrando el timestamp. Si es correcto se envía un *KRB_AS_REP*.
3) Posteriormente se realiza el proceso para solicitar un TGS, por lo que se envía al KDC un mensaje *KRB_TGS_REQ*. Entre otros, los apartados que se pueden apreciar son:
   - Nombre del usuario.
   - Timestamp.
   - TGT.
   - SPN del servicio solicitado.
   - Nonce (generado por el usuario)
4) Una vez el KDC recibe este mensaje, devuelve un mensaje *KRB_TGS_REP*. Dentro del cual, entre otros, se aprecian las siguientes partes:
   - Nombre del usuario.
   - TGS
   - Datos cifrados
5) Si todos los procesos anteriores salieron bien, el usuario ya podrá acceder al servicio deseado y para usarlo necesitará enviar un mensaje *KRB_AP_REQ*. Donde se especifica:
   - TGS
   - Datos cifrados: (que contienen la clave de sesión del servicio como nombre de usuario y timestamp para evitar ataques de replay) [2].

D. Mensajes

- **KRB_AS_REQ**: Es el mensaje realizado por el usuario para solicitar el TGT al KDC.
- **KRB_AS_REP**: Es la respuesta del KDC para enviar el TGT al usuario.
- **KRB_TGS_REQ**: Es utilizado por el usuario para solicitar el TGS al KDC, utilizando el TGT.
- **KRB_TGS_REP**: Se trata de la respuesta del KDC para enviar el TGS solicitado al usuario.
- **KRB_AP_REQ**: Es utilizado por el usuario para identificarse contra el servicio deseado, utilizando el TGS del propio servicio.
- **KRB_AP_REP**: Este mensaje es opcional y es utilizado por el servicio para autenticarse frente al usuario.
- **KRB_ERROR**: Es utilizado por los diferentes agentes para notificar situaciones de error.
- **KERB_VERIFY_PAC_REQUEST** : Es un mensaje utilizado por el AP para enviar la firma del PAC al KDC y verifica si la contraseña es correcta. No es parte de kerberos, sino de NRPC [2] [4].

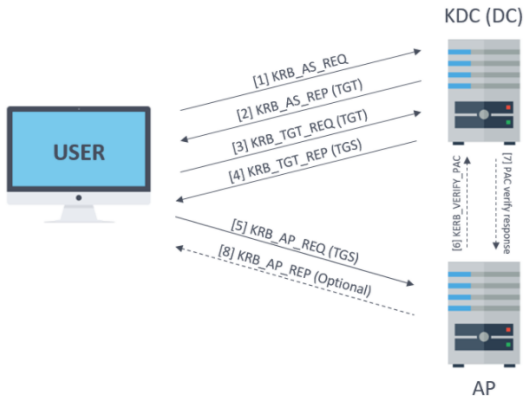

Fig. 1. Resumen de los mensajes de Kerberos

E. Indique cuál es la funcionalidad principal de Diameter e indique sus principales características. (máximo media carilla)

El protocolo Diameter proporciona servicios de mensajería de autenticación, autorización y contabilidad (AAA) para acceso a redes y aplicaciones con movilidad de datos en redes 3G, sistemas multimedia IP (IMS) y LTE/4G, deciden a qué servicios puede acceder un usuario, con qué calidad de servicio (QoS) y a qué coste. Posee ventajas como:

- Escalabilidad ilimitada para permitir el crecimiento.
- Tolerancia a fallos para garantizar la entrega de mensajes
- Apoyo a agentes para definir claramente los agentes proxy, de redireccionamiento, de retransmisión o de traducción
- Transmisión segura de paquetes de mensajes.
- Transmisión fiable a través de TCP o SCTP.

Diameter funciona de la siguiente manera, Cada host que implementa el protocolo Diameter puede actuar como cliente o servidor dependiendo de la arquitectura de la red. El nodo de Diameter que recibe la petición de conexión del usuario actuará como cliente de Diameter. Tras recibir las credenciales del usuario (nombre de usuario y contraseña), el nodo cliente envía un mensaje de petición de acceso a otro nodo de Diameter. Este nodo servidor de Diameter autentifica al usuario en función de la información proporcionada. Si la información se acepta, el usuario recibirá una respuesta de permiso de acceso a través del nodo cliente de Diameter correspondiente.

Si se rechaza, el usuario recibirá un mensaje de denegación de acceso [5].

REFERENCES

[1] "Kerberos". https://web.archive.org/web/20060314185313/http://www.ietf.org/rfc/rfc1510.txt (accedido jul. 13, 2021).

[2] "Kerberos (I): ¿Cómo funciona Kerberos? - Teoría, Tarlogic - Ciberseguridad, Ciberinteligencia y RedTeam", mar. 20, 2019. https://www.tarlogic.com/blog/como-funciona-kerberos/ (accedido jul. 13, 2021).

[3] "How the Kerberos Service Works (System Administration Guide: Security Services)". https://docs.oracle.com/cd/E19120-01/open.solaris/819-3321/intro-25/index.html ((accedido jul. 13, 2021).

[4] "What Is Kerberos, How Does It Work, and What Is It Used For?", Simplilearn.com, mar. 27, 2020. https://www.simplilearn.com/what-is-kerberos-article (accedido jul. 13, 2021).

[5] "Protocolo Diameter. https://www.f5.com/es_es/services/resources/glossary/diameter-protocol.((accedido jul. 13, 2021).