**UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA**

**UNAN-León**

****

**FACULTAD DE CIENCIAS Y TECNOLOGÍA**

**DEPARTAMENTO DE COMPUTACIÓN**

**INGENIERÍA EN TELEMÁTICA**

**COMPONENTE:** Seguridad de Redes

**DOCENTE:** Aldo Martínez

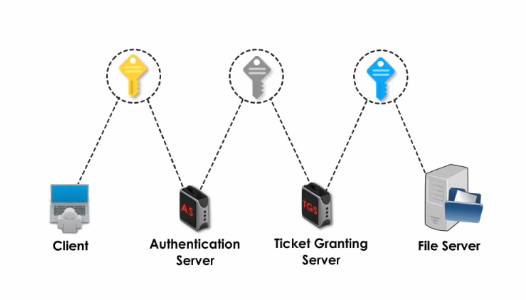
**TEMA:** Programación de Kerberos.

**FECHA:** 27/07/19

**INTEGRANTE:** Jonathan Eduardo Ochoa Velasquez 15-01898-0

¡A la libertad por la Universidad!

**¿Cuál es la arquitectura y funcionamiento de Kerberos?**



R= Kerberos es un sistema de autenticación de usuarios. Se basa en una arquitectura cliente servidor, la cual añade una 3ra entidad (Kerberos) que proporciona 2 servicios: el de autenticación (AS, Authentication Service) y el de tickets (TGS, Ticket Granting Service). Kerberos se base en criptografía simétrica, y este tiene las claves privadas de los clientes y de los servidores, los 2 servicios de Kerberos comparten una clave privada. Si un cliente quiere comunicarse con un servidor, primero debe de autenticarse, para realizar la autenticación realiza lo siguiente:

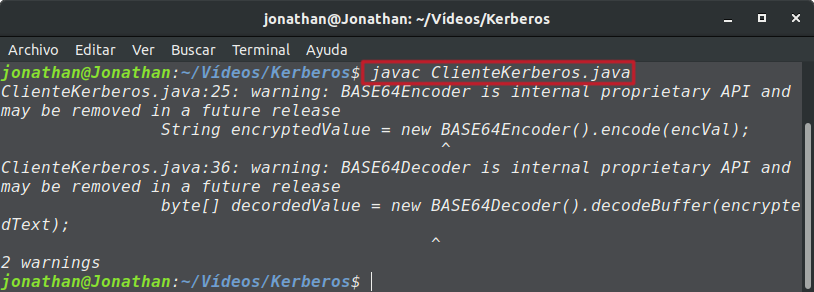
* El cliente envía una solicitud de autenticación cifrado con su clave privada al AS.
* El servicio AS recibe la petición y la descifra con la clave privada del cliente, de esta manera se asegura que el cliente es quien dice ser.
* El AS le envía al cliente un boleto cifrado con la clave compartida por los servidores Kerberos.
* El cliente le envía este boleto al TGS y le indica que quiere establecer una conexión con un servidor, el TGS así se asegura que el cliente es quien dice ser.
* El TGS le envía un token al cliente cifrado con la clave privada del servidor al que el cliente se desea conectar y una clave privada para que el cliente use con el servidor que se desea conectar, esta clave privada es enviada en el token y en otro mensaje cifrado con la clave del cliente.
* El cliente le envía ese token al servidor, el servidor descifra el token con su clave privada, asegurándose que el cliente es quien dice ser, y ya se pueden intercambiar información de forma segura por un periodo de tiempo limitado, que está indicado en el token.

Programación de Kerberos:

La aplicación no tiene interfaz, por lo que la compilación y ejecución se realizará por la terminal de Linux. Dicha aplicación consta de 4 archivos .java:

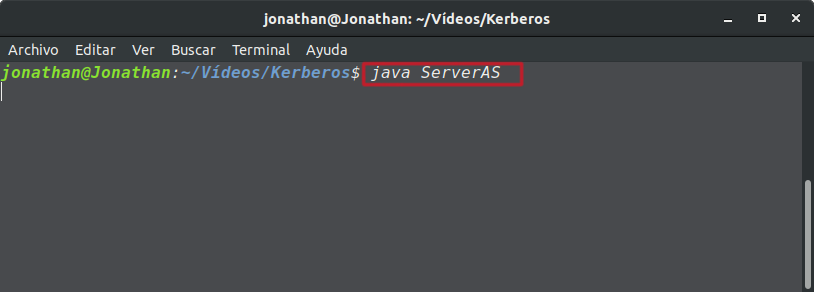
* ClienteKerberos = Cliente que realizará conexión con el servidor.
* ServerAS = Servidor Kerberos que se encarga de validar la identidad del cliente.
* ServerTGT = Servidor Kerberos que le entregará el token al cliente para que se pueda comunicar con el servidor.
* Servidor = Servidor que ofrece el servicio que el cliente desea.

Como primer paso se tienen que compilar todos los archivos .java en la terminal, para poder compilarlos se utiliza el siguiente comando:



Esto nos creará un archivo .class, que será nuestro ejecutable. Es necesario hacer esto con los 4 archivos .java

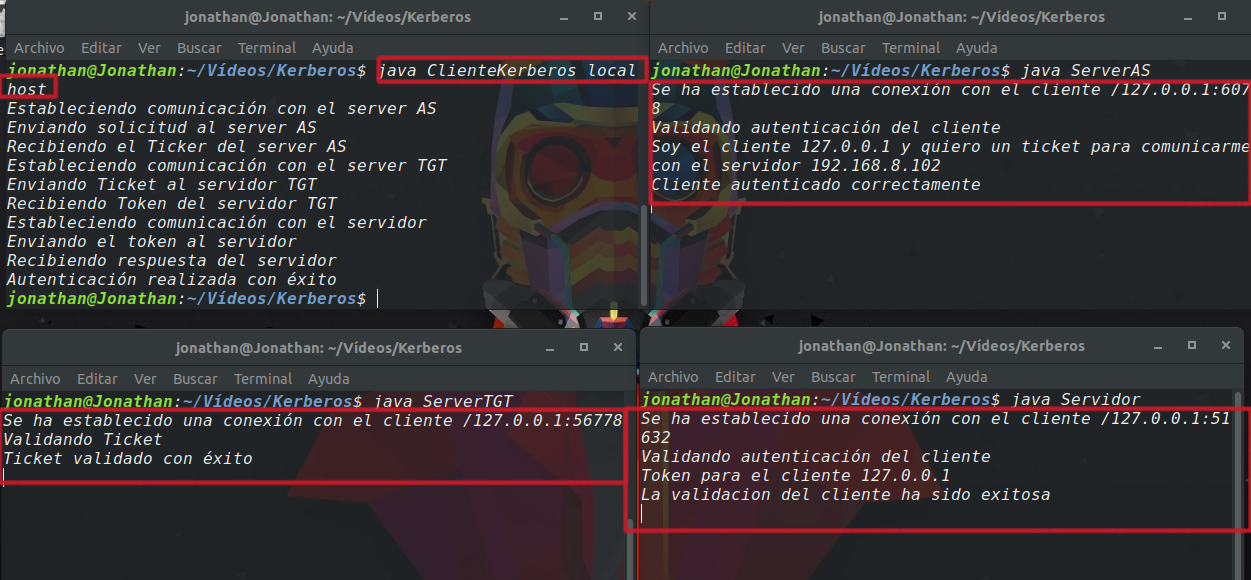
Para poder ejecutar los archivos .class se utiliza el siguiente comando:



En este caso, no se observa nada, esto es porque el servidor está esperando conexiones de los clientes.

Para la ejecución del cliente, aparte de poner java [archivo .class] se debe de especificar la dirección IP del servidor.

Ejemplo de la ejecución:



En la captura anterior podemos observar 4 terminales, cada una representa al cliente y a los 3 servidores (2 de Kerberos). Primero el cliente le envía una solicitud al serverAS y le dice que se desea comunicar con el servidor 192.168.8.102, el serverAS recibe el mensaje, lo descifra y lee el mensaje para saber con que servidor se desea comunicar el cliente, si todo está bien, el serverAS envía un Ticket al cliente, el cliente recibe el Ticket cifrado y se lo envía al serverTGT, el serverTGT descifra el ticket y le envía al cliente un token cifrado para que se pueda comunicar con el servidor, el cliente recibe el token y se lo envía al servidor, el servidor descifra el token y de esta manera se asegura de que el cliente es quien dice ser.