



Ciberseguridad

# Kerberos y sus Tickets:

La Clave para una Autenticación Segura

Concientización





# ¿Qué es Kerberos?

Kerberos es un protocolo de autenticación diseñado para entornos de red, que permite a los usuarios y servicios verificar su identidad de forma segura sin enviar contraseñas en texto plano. Es ampliamente usado en sistemas como Windows Active Directory y en redes empresariales para el inicio de sesión único (SSO).





# ¿Cómo funciona?

Kerberos usa un modelo basado en tickets y funciona con un Centro de Distribución de Claves (KDC), que es el encargado de autenticar usuarios y otorgar acceso a servicios de red.

## Proceso simplificado de autenticación:

- 1 Inicio de sesión:** El usuario ingresa su usuario y contraseña.
- 2 Ticket de Autenticación (TGT):** Si las credenciales son correctas, el KDC entrega un TGT, que es un permiso temporal cifrado.
- 3 Acceso a servicios:** Cuando el usuario quiere acceder a un servicio (por ejemplo, un servidor de archivos), usa el TGT para solicitar un ticket de servicio.
- 4 Autorización:** El servidor valida el ticket sin necesidad de que el usuario ingrese su contraseña nuevamente.

**Concientización**





# Ticket de Concesión de Tickets (TGT)

Este es el primer ticket que obtiene un usuario al autenticarse en Kerberos. Es esencialmente un "pase" que permite solicitar otros tickets sin volver a ingresar la contraseña.

- 1** El usuario ingresa su usuario y contraseña.
- 2** El KDC verifica la identidad y entrega un TGT cifrado con una clave secreta.
- 3** Mientras el TGT sea válido, el usuario puede pedir tickets para distintos servicios sin necesidad de autenticarse de nuevo.





# Ticket de Servicio (TGS)

Este ticket permite a un usuario acceder a un servicio específico dentro de la red (por ejemplo, un servidor de archivos o una base de datos).

- 1** El usuario usa su TGT para solicitar un TGS al KDC.
- 2** El KDC verifica el TGT y entrega un TGS cifrado, válido solo para el servicio solicitado.
- 3** El usuario presenta el TGS al servidor del servicio, que lo valida y otorga acceso.
  - Evita que se reenvíen contraseñas, ya que solo usa tickets cifrados.
  - Es válido solo para un servicio específico, reduciendo el riesgo de abuso.



# Ticket de Delegación

En algunos casos, un servicio puede necesitar acceder a otro en nombre del usuario. Kerberos permite esto mediante la delegación de tickets.

## Tipos de delegación:

- **Delegación Confiada:** Un servicio puede solicitar tickets en nombre del usuario sin restricciones.
- **Delegación Restringida:** Solo puede delegar el acceso a servicios específicos.

### Ejemplo

Un servidor web autenticado con Kerberos puede necesitar acceder a una base de datos en nombre del usuario sin pedirle su contraseña nuevamente.

### Concientización





# Ataques contra Kerberos

- ✖ **Pass-the-Ticket:** Robo de tickets de autenticación para suplantar identidad.
- ✖ **Golden Ticket:** Un atacante con acceso al KDC puede generar tickets falsos.
- ✖ **Kerberoasting:** Extracción de hashes de contraseñas de cuentas de servicio.



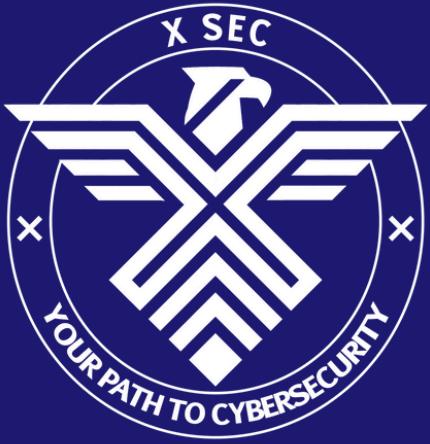


# ¿Cómo proteger Kerberos?

- Usa contraseñas seguras y gestiona cuentas de servicio con contraseñas largas.
- Implementa detección de anomalías en autenticaciones.
- Habilita cifrado fuerte y autenticación multifactor (MFA) si es posible.

Concientización





Ciberseguridad

# Seguinos y únete al discord para seguir aprendiendo

 Guardar

 Compartir

 Seguir

Concientización

Save