Seguridad LAN en entornos Ethernet

Configuridad de seguridad básica en Switches

- Contraseñas Seguras
  - Se debe usar siempre la opción secret, además de letras números y caracteres especiales.
  - Activar “service password-encryption” para evitar que las contraseñas se puedan descubrir mirando la configuración.
  - Utilizar gestión de usuarios AAA:
- Configuración de advertencias: Propósito disuasivo
  - “banner motd” o “banner login” como mensaje previo a la autenticación
  - Tanto para fines legales como administrativos, se configura un mensaje de advertencia.
- Acceso seguro a la consola: seguridad física y lógica configurando el control de acceso
- Acceso Seguro a través de líneas VTY:
  - Usar SSH2 en vez de telnet
  - Aplicar ACLs a las líneas VTY para limetar el acceso a solo las estaciones de gestión desde ciertas subredes. Se limita el acceso administrativo a determinadas IPs origen.
  - Uso de control de acceso AAA-NewModel
- Deshabilitar daemon HTTP:
  - Se recomienda su desactivación o, si no es posible, activar el modo HTTP secure con : “ip http secure-server”
  - Configurar ACLs para permitir acceso SOLO desde redes seguras.
- Deshabilitar servicios innecesarios
- Utilización de SNMPv3 con autenticaciín y privacidad y ACLs para limitar el acceso SNMP a las estaciones de trabajo y subredes de confianza

Asegurar topología de Spanning-Tree

From:
https://knoppia.net/ - **Knoppia**

Permanent link:
https://knoppia.net/doku.php?id=redes:segether&rev=1729265484

Last update: **2024/10/18 15:31**