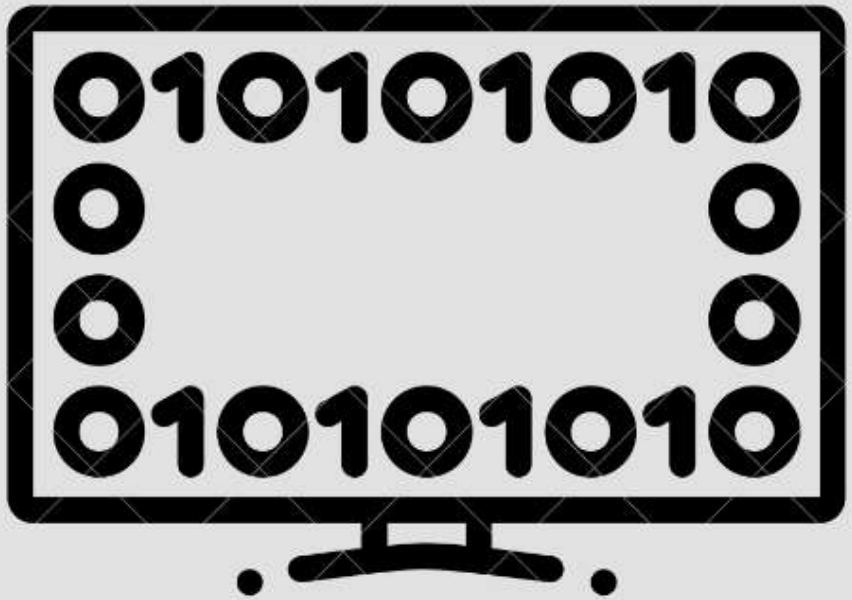

CONTROL DE ACCESO
Telnet

INTRODUCCIÓN A TELNET:

Telnet es un protocolo de red que permite la comunicación entre dispositivos a través de una interfaz de texto. Utiliza el modelo cliente-servidor y opera sobre el protocolo TCP/IP. La característica principal de Telnet es proporcionar un acceso remoto a sistemas y dispositivos para administración y configuración mediante una sesión de terminal virtual.



RIESGOS DE TELNET:

Aunque Telnet es una herramienta útil para el acceso remoto, tiene limitaciones significativas en términos de seguridad. La información transmitida a través de Telnet, incluyendo contraseñas y comandos, se envía en texto plano, lo que la hace vulnerable a la interceptación y visualización por parte de usuarios no autorizados.


CONTROL DE ACCESO EN TELNET:
Para mitigar los riesgos asociados con el uso de Telnet, es esencial implementar medidas de control de acceso. Estas medidas están diseñadas para limitar quién puede acceder a un dispositivo a través de Telnet y cómo se puede acceder.

MEDIDAS:

Contraseñas de Acceso:

- Se establecen contraseñas sólidas para autenticar a los usuarios durante la conexión Telnet.
- La complejidad de las contraseñas, incluyendo longitud y caracteres especiales, se configura para fortalecer la seguridad.

Listas de Control de Acceso (ACL):

- Se utilizan listas de control de acceso para especificar qué direcciones IP o rangos tienen permitido el acceso Telnet.
- Pueden ser configuradas para permitir o denegar el acceso basado en la dirección IP de origen.

Desactivar Telnet:

- En entornos donde la seguridad es prioritaria, se desactiva Telnet en favor de protocolos más seguros como SSH.
- Desactivar Telnet reduce la exposición a amenazas de seguridad inherentes al protocolo.

FUNCIONAMIENTO DEL PROTOCOLO TELNET

1. Establecimiento de la Conexión:
   - El cliente Telnet inicia una solicitud de conexión al servidor Telnet especificando el puerto estándar (generalmente el puerto 23).
   - La conexión se establece utilizando el protocolo TCP.
2. Sesión de Terminal Virtual:
   - Una vez establecida la conexión, se inicia una sesión de terminal virtual en el servidor.
   - La sesión permite al usuario interactuar con el sistema remoto como si estuviera físicamente presente en el mismo.
3. Negociación de Opciones:
   - Telnet permite la negociación de diversas opciones entre el cliente y el servidor durante el establecimiento de la conexión.
   - Estas opciones pueden incluir configuraciones de terminal, manipulación de caracteres especiales, entre otras.

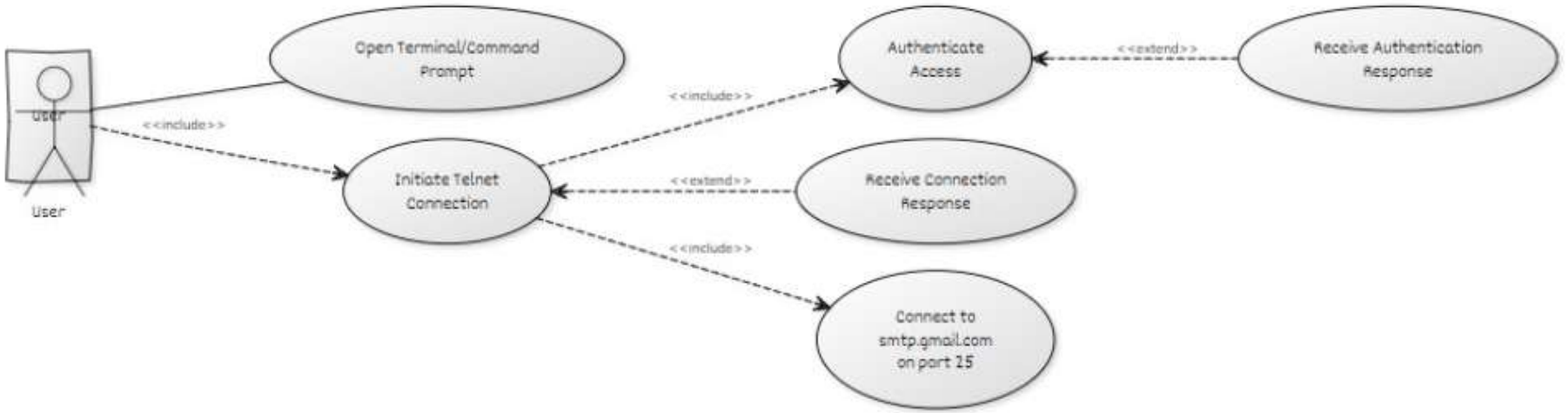
CONTINUACION

4. Flujo de Datos en Texto Plano:
   - Telnet transmite datos en formato de texto plano.
   - Cada carácter ingresado por el usuario se envía al servidor Telnet, y la respuesta del servidor se muestra en la terminal del cliente.
5. Autenticación:
   - La autenticación se realiza mediante el intercambio de nombres de usuario y contraseñas.
   - Es crítico implementar contraseñas seguras para evitar la interceptación de credenciales durante la transmisión.
6. Control de Acceso - Listas de Control de Acceso (ACL):
   - Se utilizan listas de control de acceso para permitir o denegar el acceso a usuarios basándose en direcciones IP o rangos específicos.
   - Esto puede ser implementado tanto en el lado del cliente como en el servidor.

CONTINUACION

7. Seguridad Limitada:
   - Telnet no proporciona cifrado de datos, lo que significa que la información, incluidas las contraseñas, se transmite en texto plano.
   - Para mejorar la seguridad, algunas implementaciones permiten utilizar Telnet sobre SSH, lo que agrega una capa de cifrado a la conexión.
8. Desactivación de Telnet y Transición a SSH:
   - Dada la vulnerabilidad de Telnet a ataques de escucha y captura, en entornos críticos, se desactiva Telnet en favor de protocolos más seguros como SSH.
   - SSH ofrece cifrado fuerte y autenticación mejorada, proporcionando una capa adicional de seguridad.
9. Implementación de Medidas de Seguridad Adicionales:
   - Además de la autenticación y el control de acceso, se pueden implementar medidas como la auditoría de eventos para rastrear actividades y alertar sobre posibles intrusiones.

EJEMPLO:


Open Terminal/Command Prompt
Authenticate Access
<<extend>>
Receive Authentication Response
User
<<include>>
<<include>>
Initiate Telnet Connection
<<extend>>
Receive Connection Response
<<include>>
Connect to smtp.gmail.com on port 25
User


¡MUCHAS GRACIAS!
yepetos