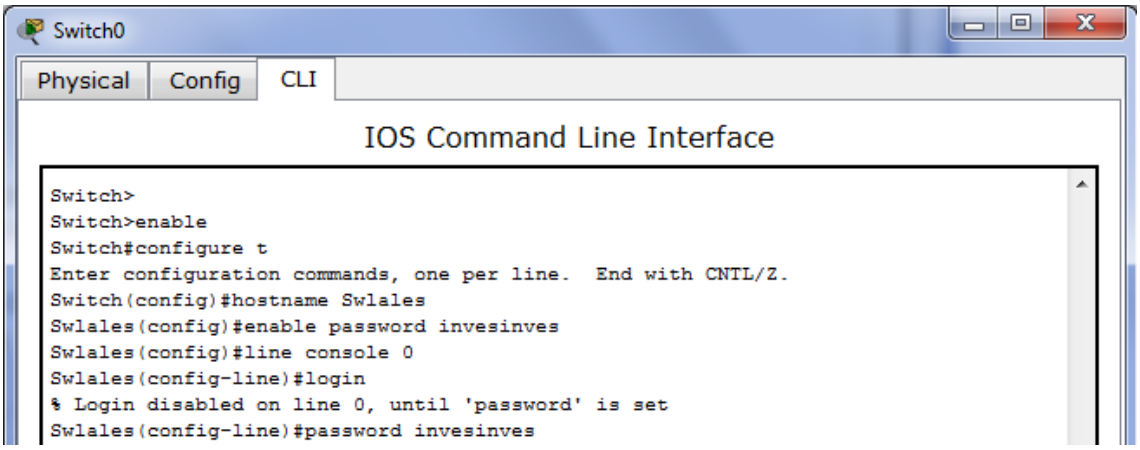
ACTIVIDAD 6 - RIESGOS POTENCIALES EN LOS SERVICIOS DE RED – TEMA 2

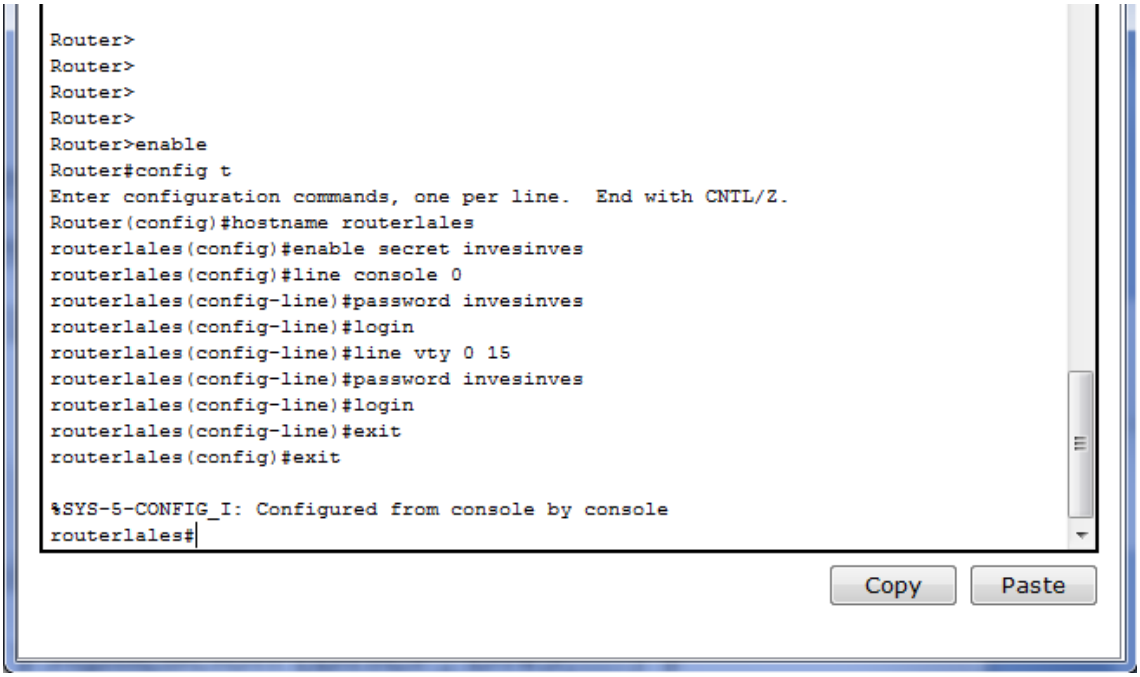
a) Configura en modo seguro un switch CISCO (Packet Tracer)

Entramos en Packet Tracer y cogemos un switch y lo configuramos de la siguiente forma



b) Configura en modo seguro un router CISCO

Entramos en Packet Tracer y cogemos un router y lo configuramos de la siguiente forma



c) Elabora un documento que manifieste las vulnerabilidades en las capas enlace, red (IP), TCP-UDP y Aplicación (DHCP, DNS,….) y como protegerse de las mismas.

Las principales amenazas en la capa de aplicación son:

Ataques que usan ARP Spoofing:
Switch Port Stealing (Sniffing): Utilizando ARP Spoofing el atacante consigue que todas las tramas dirigidas hacia otro puerto del switch lleguen al puerto del atacante para luego reenviarlos hacia su destinatario y de esta manera poder ver el tráfico que viaja desde el remitente hacia el destinatario (Una especie de Sniffing half-duplex).

Man in the Middle (Sniffing): Utilizando ARP Spoofing el atacante logra que todas las tramas que intercambian las víctimas pasen primero por su equipo (Inclusive en ambientes switcheados) **Secuestro (Hijacking):** Utilizando ARP Spoofing el atacante puede lograr redirigir el flujo de tramas entre dos dispositivos hacia su equipo. Así puede lograr colocarse en cualquiera de los dos extremos de la comunicación (previa deshabilitación del correspondiente dispositivo) y secuestrar la sesión.

Denial of service (DoS): Utilizando ARP Spoofing el atacante puede hacer que un equipo crítico de la red tenga una dirección MAC inexistente. Con esto se logra que las tramas dirigidas a la IP de este dispositivo se pierdan.

POSIBLES SOLUCIONES

Seguridad inalámbrica: La seguridad en las redes inalámbricas es sumamente importante, por la facilidad con que cualquiera puede encontrarlas y acceder a ellas. Cualquier persona con un ordenador portátil puede encontrar fácilmente el punto de acceso inalámbrico de nuestra red inalámbrica, pudiendo así ingresar en nuestros archivos, utilizar nuestra conexión a internet, obtener datos importantes que se transfieran en la red inalámbrica, etc. Por ejemplo, la ausencia de seguridad en nuestra red inalámbrica o nuestro punto de acceso a internet inalámbrico puede hacernos víctimas del piggybacking, del phishing, del robo de información, etc.

Vulnerabilidades de la capa de red

Las vulnerabilidades de esta capa están asociadas a los medios sobre los cuales se realiza la conexión. Esta capa presenta problemas de control de acceso y de confidencialidad. Ejemplos de estas vulnerabilidades son desvió de los cables de conexión hacia otros sistemas, pinchazos de la línea, escuchas en medios de transmisión inalámbricos, etc.

Espionaje En general, la mayoría de las comunicaciones por red tienen lugar en formato de texto simple (sin cifrar), lo que permite al atacante que haya logrado el acceso a las rutas de datos de una red observar e interpretar (leer) el tráfico. El espionaje de las comunicaciones por parte de un atacante se conoce como husmear. La capacidad de los espías para observar la red suele ser el mayor problema de seguridad que afrontan los administradores de las compañías. Sin unos servicios de cifrado eficaces basados en criptografía, mientras los datos atraviesan la red pueden ser observados por terceros.

Modificación de datos Cuando un atacante ha leído los datos, a menudo el siguiente paso lógico consiste en modificarlos. Un atacante puede modificar los datos de un paquete sin que el remitente ni el receptor lo adviertan. Incluso cuando no se requiera confidencialidad en todas las comunicaciones, no se desea que los mensajes se modifiquen en su camino. Por ejemplo, si intercambia solicitudes de compra, no desea que se modifique la información relativa a los artículos, los importes ni la facturación.

Vulnerabilidades de la capa Internet

En esta capa se puede realizar cualquier tipo de ataque que afecte a un datagrama IP. Tipos de ataques que se pueden realizar en esta capa son por ejemplo: técnicas de Sniffing o escuchas de red, suplantación de mensajes, modificación de datos, retrasos de mensajes y denegación de mensajes. Cualquier atacante puede suplantar un paquete si indica que proviene de otro sistema. La suplantación de un mensaje se puede realizar por ejemplo dando una respuesta a otro mensaje antes de que lo haga el suplantado. La autentificación de los paquetes se realiza a nivel de máquina por dirección IP y no a nivel de usuario. Si un sistema da una dirección de maquina errónea, el receptor no detectara la suplantación. Este tipo de ataques suele utilizar técnicas como la predicción de números de secuencia TCP, el envenenamiento de tablas cache, etc.

Vulnerabilidades de la capa de transporte

Esta capa trasmite información TCP o UDP sobre datagramas IP. En esta capa se pueden encontrar problemas de autentificación, integridad y de confidencialidad. Los ataques más conocidos en esta capa son la denegación de servicio de protocolos de transporte. En el mecanismo de seguridad del diseño del protocolo TCP, existe una serie de ataques que aprovechas las deficiencias en el diseño, entre las más graves se encuentra la posibilidad de la intercepción de sesiones TCP establecidas, con el objetivo de secuestrarlas y dirigirlas a otros equipos.

MARÍA ÁNGELES PEÑASCO SÁNCHEZ- ACTIVDAD 6 – TEMA 2