Video: Métodos de acceso seguro (9 min)

Una de las primeras acciones que querrá hacer al instalar un dispositivo en su red, como un switch Cisco Series, es tener acceso seguro al dispositivo por lo que solo un administrador podrá configurarlo o cambiar sus configuraciones. Para ello, deberemos establecer algunos ajustes de configuración inicial para el acceso seguro. Haré clic en la PC de escritorio y clic en el programa de emulación de terminal, y podrán ver que ahora tengo una conexión de consola al switch.

Para este video, usaré la interfaz de línea de comandos directamente al switch. Como pueden observar, estoy registrado en el switch en el modo exec de usuario sin ninguna autenticación. Esto representa un riesgo de seguridad. Un riesgo de seguridad aún mayor es qué puedo escribir el comando habilitado y acceder al modo exec privilegiado. también sin ningún tipo de autenticación o contraseña. En el modo exec privilegiado, puedo iniciar la configuración del switch, por lo que lo primero que querrá hacer será asegurar el acceso al modo exec privilegiado.

Para ello, iré al modo de configuración global e ingresaré el comando "enable secret" y luego la contraseña. querrá usar contraseñas seguras y complejas siempre que sea posible. Dado que se trata de una prueba de caso, utilizaré la contraseña "class." El parámetro "secret" me asegura que la contraseña "class" será cifrada en el archivo de configuración. Una alternativa de este comando es "enable password class." Esta alternativa del comando no proporciona cifrado para la contraseña dentro del archivo de configuración. Pulsaré la tecla de retroceso en el comando. Veamos si nuestra clase de contraseña secreta habilitada funcionó. Haré Ctrl+C para acceder al modo exec privilegiado y luego salir del switch. Ahora presionaré Enter. Ahora me encuentro en el modo exec con privilegios. Escribiré "enable", y pueden ver que me piden la contraseña. Cuando escribo la contraseña, no podrá ver ninguno de los caracteres que escribo. Escribiré "class" y presionaré Enter, y podrán ver que ahora me encuentro en el modo exec con privilegios.

Analicemos nuestra configuración en ejecución hasta este punto. Podemos hacer esto escribiendo en el comando "show running-config" para ver nuestra configuración en ejecución. Presionaré Enter, y podrán ver aquí en la parte superior, que se encuentra nuestro comando "enable secret". El 5 significa que hay un hash MD5, y es un hash unidireccional de nuestra contraseña "class". Pueden ver cómo el comando "enable secret" ofusca la contraseña dentro del archivo de configuración. Para ver el resto de su archivo de configuración, debe pulsar la barra espaciadora en el teclado. Ahora hemos cifrado la "enable password" o el acceso al modo exec privilegiado, pero ¿qué pasa con el acceso para trabajar simplemente con la consola en el switch? También podemos asegurar eso. Para hacerlo, escribiré "enable", la contraseña "class", tendré acceso al modo de configuración global con el comando "conf t", y deberé entrar al modo de configuración de línea para line console 0. Escribiré "line console 0", y ahora me encuentro en el modo de configuración de línea. Ahora puedo ingresar una contraseña para mi conexión de consola. escribiré "password", normalmente usaría una contraseña compleja, pero para esta demostración, utilizaré simplemente la contraseña "cisco" y presionaré Enter. Escribiré en el comando "login", que habilita el inicio de sesión del administrador global en la consola de línea 0. Ahora que he asegurado el puerto de consola, también querré asegurar el acceso de terminal virtual para inicios de sesión remotos. escribiré "line vty" para la terminal virtual o teletipo virtual, y luego cuántas líneas quiero permitir al acceso remoto. El switch Cisco tiene una capacidad de hasta 16 inicios de sesión remotos simultáneos a través de los terminales virtuales. Para configurar los 16, simplemente escribo 0 para la primera terminal, un espacio y luego la terminal más reciente que quiero configurar. En este caso, pondré 15. Esto me permitirá configurar los terminales virtuales 0 a 15. Pondré "password cisco", y luego el comando inicio de sesión.

Veamos estas contraseñas en nuestra configuración en ejecución. Para hacerlo, haré Ctrl+C para acceder al modo exec privilegiado, y luego pondré el comando "show run" abreviación para "show running-config." Presionaré la tecla tabulación y podrá ver el comando completo. Aquí está el archivo de configuración en ejecución. Presionaré la barra espaciadora y me dirigiré hacia la parte inferior, podrán ver que están las configuraciones para line con 0, line vty 0 a 4, y line vty 5 a 15. El IOS divide las líneas de terminal virtual en dos grupos: 0 a 4 y 5 a 15. Observe que la contraseña "cisco" está en texto no cifrado. Es distinta que la "contraseña enable secret", que se ha cifrado a través de un hash unidireccional. Podemos agregar mayor seguridad al switch si podemos cifrar estas contraseñas de manera tal que no sean más visibles en textos sin formato y claros.

Para ello, volveré al modo global de configuración y pondré el comando "service password-encryption." Este comando colocará un nivel liviano de cifrado en todas las contraseñas en el switch. Podemos ver esta opción si volvemos al modo exec privilegiado, observemos el archivo de configuración en ejecución... Presionaré la barra espaciadora hasta la parte inferior, y podrán ver que ahora la contraseña "cisco" se ha cifrado con un cifrado tipo 7. Esta no es una manera muy sólida de cifrado, pero agrega una capa de seguridad. Otro comando de configuración inicial importante para asegurar el acceso al switch es mediante la configuración un mensaje de aviso. Para ello, iré al modo de configuración global y escribiré en el comando "banner motd" para el "mensaje del día." Ahora podré ingresar un mensaje que se presentará a los usuarios cuando inicien sesión. Este mensaje servirá como advertencia legal para usuarios no autorizados informándoles que están violando el acceso y se tomarán acciones legales. ahora puedo ingresar mi mensaje de seguridad. El mensaje que escribo deberá estar entre dos delimitadores. Es recomendable usar un delimitador que no sea un carácter dentro del mensaje. Por ejemplo, usaré comillas como delimitadores para mi mensaje. Entre los signos de interrogación, pondré el mensaje "¡No se permite el acceso no autorizado, los infractores serán procesados con el máximo rigor de la ley!" Esto permite a cualquier supuesto hacker saber que están violando un dispositivo seguro o red segura y que se trata de un entorno protegido ejecutorio por la ley. Presionaré Enter y se configura el anuncio. Ahora observemos algunas de estas configuraciones de seguridad. Haré Ctrl+C; escribiré "exit" para salir del switch. Presionaré Enter. Observen que aparece el anuncio de advertencia además de una solicitud de contraseña solo para tener acceso a la consola. Pondré la contraseña "cisco", y ahora me encuentro en el modo exec del usuario. Escribiré "enable." Ahora me solicitan otra contraseña para alcanzar al modo exec privilegiado. Escribiré la contraseña "class", y ahora dispongo de acceso total al switch.