

Práctica de práctica de laboratorio: Investigación de procedimientos de recuperación de contraseña (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Parte 1: Investigar el registro de configuración

- Identificar el propósito del registro de configuración.
- Describir el comportamiento del router para distintos valores del registro de configuración.

Parte 2: Registrar el procedimiento de recuperación de contraseña para un router Cisco específico

- Investigar y registrar el proceso de recuperación de contraseñas en un router Cisco específico.
- Responder las preguntas sobre la base del procedimiento investigado.

Información básica/Situación

El propósito de esta práctica de laboratorio es investigar el procedimiento para recuperar o restablecer la contraseña de enable en un router Cisco específico. La contraseña de enable protege el acceso al modo EXEC privilegiado y al modo de configuración en los dispositivos Cisco. La contraseña de enable se puede recuperar, pero la contraseña secreta de enable está encriptada y debe reemplazarse por una contraseña nueva.

Para omitir una contraseña, el usuario debe estar familiarizado con el modo monitor ROM (ROMMON), así como con los parámetros del registro de configuración para los routers Cisco. ROMMON es el software básico de CLI almacenado en la ROM, que se puede utilizar para resolver problemas de errores de arranque y para recuperar un router cuando no se encuentra un IOS.

En esta práctica de laboratorio, comenzará investigando el propósito del registro de configuración para los dispositivos Cisco y los parámetros de dicho registro. Luego, investigará y detallará el procedimiento exacto para la recuperación de la contraseña en un router Cisco específico.

Recursos necesarios

- Dispositivo con acceso a Internet

Parte 1: Investigar el registro de configuración

Para recuperar o restablecer una contraseña de enable, un usuario utiliza la interfaz ROMMON para instruir al router que omita la configuración de inicio durante el arranque. Una vez que se arranca el dispositivo, el usuario accede al modo EXEC privilegiado, sobrescribe la configuración en ejecución con la configuración de inicio guardada, recupera o restablece la contraseña, y restaura el proceso de arranque del router para que incluya la configuración de inicio.

El registro de configuración del router desempeña un papel fundamental en el proceso de recuperación de contraseñas. En la primera parte de esta práctica de laboratorio, investigará el propósito del registro de configuración de un router y el significado de ciertos valores de dicho registro.

Nota para el instructor: los estudiantes deben visitar la página **Use of Configuration Register on All Cisco Routers** (Uso del registro de configuración en todos los routers Cisco) en el sitio Web de Cisco http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a008022493f.shtml.

Paso 1: Describir el propósito del registro de configuración

¿Cuál es el propósito del registro de configuración?

El registro de configuración se puede utilizar para cambiar la forma en que arranca el router, las opciones de arranque y la velocidad de la consola.

¿Qué comando cambia el registro de configuración en el modo de configuración?

config-register

¿Qué comando cambia el registro de configuración en la interfaz ROMMON?

confreg

Paso 2: Determinar los valores del registro de configuración y sus significados

Investigue y detalle el comportamiento del router para los siguientes valores del registro de configuración.

0x2102

Para el valor 0x2102 del registro de configuración, un router carga el IOS desde memoria flash y después carga la configuración de inicio desde la NVRAM, si estuviera presente. Si no se encuentra ningún sistema operativo, el router arranca en ROMMON.

0x2142

Para el valor 0x2142 del registro de configuración, un router carga el IOS desde la memoria flash, omite la configuración de inicio en la NVRAM y proporciona una petición de entrada para el cuadro de diálogo de configuración inicial. Si no se encuentra ningún sistema operativo, el router arranca en ROMMON.

¿Cuál es la diferencia entre estos dos valores del registro de configuración?

El parámetro 0x2102 es para el funcionamiento normal del router. El parámetro 0x2142 omite la configuración de inicio al permitirle a un usuario recuperar o restablecer la contraseña de enable.

Parte 2: Registrar el procedimiento de recuperación de contraseña para un router Cisco específico

En la parte 2, describirá el procedimiento exacto para recuperar o restablecer una contraseña de un router Cisco específico y responderá preguntas sobre la base de la investigación realizada. El instructor le proporcionará el modelo exacto de router que debe investigar.

Nota para el instructor: los estudiantes deben visitar la página **Password Recovery Procedures** (Procedimientos de recuperación de contraseñas) en el sitio Web de Cisco http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml para conocer los procedimientos pertinentes para una variedad de dispositivos Cisco.

Paso 1: Detallar el proceso de recuperación de una contraseña en un router Cisco específico

Investigue y detalle los pasos y los comandos que necesita para recuperar o restablecer la contraseña de enable o la contraseña secreta de enable en su router Cisco. Resuma los pasos con sus propias palabras.

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and extend across the width of the page. There are no margins, text, or other markings on the paper.

Para recuperar o restablecer la contraseña de enable en el router Cisco serie 1900, se deben seguir estos pasos:

1. Establecer una conexión de terminal con el router utilizando Tera Term u otro emulador de terminal.
2. Arrancar en modo ROMMON, ya sea por medio de eliminar la memoria flash y reiniciar, o presionando Alt-b durante el reinicio.
3. Escribir **confreg 0x2142** en la petición de entrada de ROMMON.
4. Escribir **reset** en la siguiente petición de entrada de ROMMON.
5. Escribir **no** en el cuadro de diálogo de configuración inicial.
6. Escribir **enable** en la petición de entrada del router.
7. Escribir **copy startup-config running-config** para cargar la configuración de inicio.
8. Escribir **show running-config**.
9. Registrar una contraseña de enable sin encriptar. Restablecer una contraseña de enable encriptada.
10. En el modo de configuración, escribir **config-register 0x2102**.
11. En el modo privilegiado, escribir **copy running-config startup-config** para guardar la configuración.
12. Utilizar el comando **show version** para verificar los parámetros del registro de configuración.

Paso 2: Responder las preguntas sobre el procedimiento de recuperación de contraseñas

Utilice el proceso de recuperación de contraseñas para responder las siguientes preguntas.

Describa cómo buscar los parámetros actuales del registro de configuración.

El comando **show version** proporciona los parámetros actuales del registro de configuración.

Describa el proceso para ingresar al modo ROMMON.

Un usuario puede quitar la memoria flash y reiniciar el router para que arranque en la utilidad ROMMON. El usuario también puede arrancar el router y presionar **alt+b** si utiliza Tera Term.

¿Qué comandos necesita para acceder a la interfaz de ROMMON?

Un usuario debe introducir **confreg 0x2142** para cambiar los parámetros de configuración, seguido por **reset** para reiniciar el router.

¿Qué mensaje esperarías ver cuando arranque el router?

Si un router no carga la configuración de inicio, el usuario debería esperar ver el mensaje “Continue with configuration dialog?” (“¿Desea continuar con el cuadro de diálogo de configuración?”).

¿Por qué es importante cargar la configuración de inicio en la configuración en ejecución?

Cargar la configuración de inicio en la configuración en ejecución asegura que la configuración de inicio original permanezca intacta si el usuario realiza un guardado durante el proceso de recuperación de contraseña.

¿Por qué es importante volver a cambiar el registro de configuración al valor original después de recuperar la contraseña?

Devolver el registro de configuración a su valor original asegura que el router cargue la configuración de inicio durante la recarga siguiente.

Reflexión

1. ¿Por qué es de suma importancia que un router esté protegido físicamente para impedir el acceso no autorizado?

El procedimiento de recuperación de contraseñas se basa en una conexión de consola, lo que requiere acceso físico directo al dispositivo. Por esta razón, impedir el acceso de usuarios no autorizados al dispositivo físico es una parte fundamental del plan de seguridad general.