Sistema de evaluación

Saltar a Tiempo restante | Saltar a Navegación | Saltar a Temas de la evaluación

Comenzar la evaluación - EWAN Chapter 4 - CCNA Exploration: Acceso a la WAN (Versión 4.0)

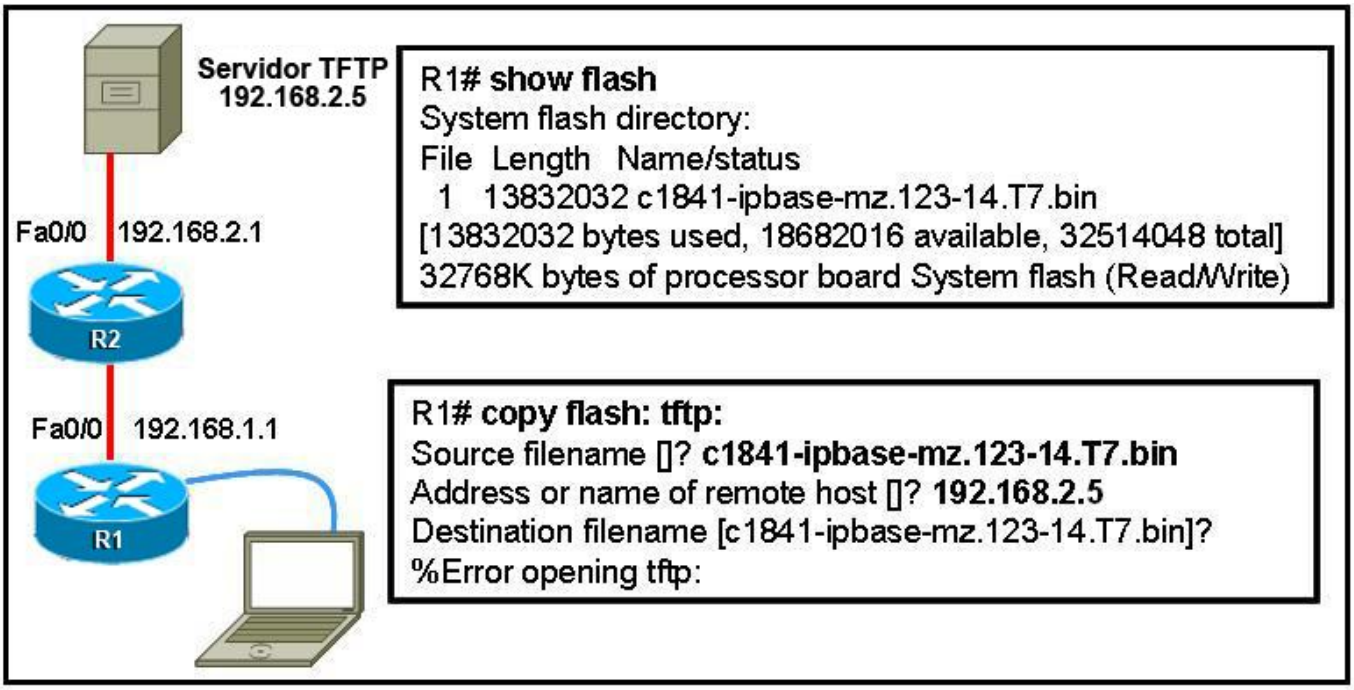
Tiempo restante: 00:39:10

Mostrando 1 de 2 Siguiente> Página: 1 IR <Ant.

1 Los usuarios no pueden obtener acceso a un servidor de la empresa. Los registros del sistema muestran que el servidor está funcionando lentamente porque recibe un alto nivel de solicitudes de servicio falsas. ¿Qué tipo de ataque se está produciendo?

- reconocimiento
- acceso
- DoS
- gusano
- virus
- caballo de Troya

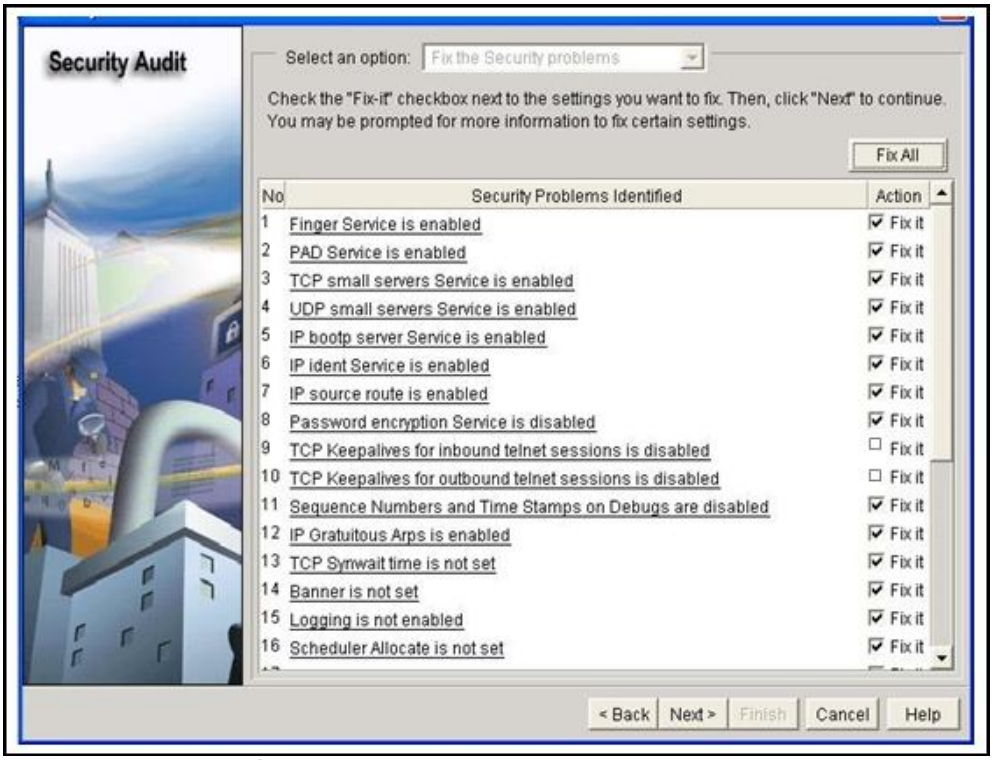
2



Consulte la ilustración. El administrador de red está intentando hacer una copia de seguridad del software del router IOS de Cisco y recibe este resultado. ¿Cuáles de las siguientes son dos posibles causas para este resultado? (Elija dos opciones).

- [ ] El archivo del IOS de Cisco tiene una check sum que no es válida.
- [ ] El cliente TFTP del router está dañado.
- [x] El router no se puede conectar al servidor TFTP.
- [x] No se inició el software del servidor TFTP.
- [ ] En el servidor TFTP no hay espacio suficiente para el software.

3



Consulte la ilustración. El Administrador de dispositivos de seguridad (SDM, Security Device Manager) se ha utilizado para configurar un nivel requerido de seguridad en el router. ¿Qué se logra cuando SDM aplica el próximo paso sobre los problemas de seguridad identificados en el router?

- SDM invocará automáticamente el comando AutoSecure.
- SDM generará un informe que marcará las acciones de configuración adecuadas para aliviar los problemas de seguridad.
- SDM creará un archivo de configuración que puede copiarse y pegarse en el router para volver a configurar los servicios.
- SDM volverá a configurar los servicios que se marcan en las ilustraciones como "solucionarlo" a fin de aplicar los cambios de seguridad sugeridos.

4

```
R1(config)# no service tcp-small-servers
R1(config)# no service udp-small-servers
```

Consulte la ilustración. ¿Qué se logra cuando ambos comandos están configurados en el router?

- Los comandos filtran el tráfico de UDP y de TCP que se dirige al router.
- Los comandos deshabilitan las solicitudes de TCP o UDP enviadas por los protocolos de enrutamiento.
- Los comandos deshabilitan los servicios como echo, discard y chargen en el router a fin de evitar las vulnerabilidades de seguridad.
- Los comandos deshabilitan los servicios de servidores BOOTP y TFTP a fin de evitar las vulnerabilidades de seguridad.

5 ¿En qué modo operativo comienza el proceso de recuperación de contraseña y qué tipo de conexión usa? (Elija dos opciones).

- [x] monitor de la ROM
- [ ] ROM de arranque
- [ ] IOS de Cisco
- [x] conexión directa a través del puerto de consola
- [ ] conexión de red a través del puerto Ethernet
- [ ] conexión de red a través del puerto serial

6 ¿En qué etapa de la Rueda de seguridad se produce la detección de intrusos?

- seguridad
- control

- prueba
- perfeccionamiento
- reconocimiento

7 ¿Cuál de las siguientes afirmaciones es verdadera con respecto al administrador de dispositivos de seguridad (SDM, Security Device Manager) de Cisco?
- SDM puede ejecutarse únicamente en routers de la serie Cisco 7000.
- SDM puede ejecutarse desde la memoria del router o desde una PC.
- SDM debe ejecutarse para configuraciones de routers complejas.
- SDM es compatible con cada versión del software IOS de Cisco.

8 ¿Cuáles de las siguientes son tres características de una buena política de seguridad? (Elija tres opciones).
- [x] Define los usos aceptables y no aceptables de los recursos de la red.
- [x] Comunica consenso y define funciones.
- [ ] Está desarrollada por usuarios finales.
- [ ] Se desarrolla una vez que todos los dispositivos de seguridad han sido completamente probados.
- [x] Define la manera de manejar los incidentes de seguridad.
- [ ] Debe estar encriptada, ya que contiene copias de seguridad de todas las contraseñas y claves importantes.

9 ¿Cuáles de los siguientes son dos afirmaciones que definen el riesgo de seguridad cuando se habilitan los servicios DNS en la red? (Elija dos opciones).
- [x] Las consultas de nombre se envían de manera predeterminada a la dirección de broadcast 255.255.255.255.
- [ ] Las consultas de nombre DNS requieren que el comando **ip directed-broadcast** esté habilitado en las interfaces Ethernet de todos los routers.
- [ ] El uso del comando de configuración global **ip name-server** en un router habilita los servicios DNS en todos los routers de la red.
- [x] El protocolo DNS básico no proporciona garantía de integridad o de autenticación.
- [ ] La configuración del router no proporciona la opción de instalar servidores DNS principales y de respaldo.

10 ¿Cuáles de las siguientes opciones son dos beneficios derivados de utilizar AutoSecure de Cisco? (Elija dos opciones).
- [ ] Le otorga al administrador un control detallado mediante el cual se activan o desactivan los servicios.
- [x] Ofrece la capacidad de desactivar instantáneamente los servicios y procesos no esenciales del sistema.
- [ ] Configura automáticamente el router para que funcione con SDM.
- [ ] Garantiza una máxima compatibilidad con otros dispositivos de su red.
- [x] Permite al administrador configurar políticas de seguridad sin la necesidad de comprender todas las características del software IOS de Cisco.

11 ¿Cuáles de las siguientes so dos afirmaciones verdaderas con respecto a la seguridad de la red? (Elija dos opciones).
- [ ] Asegurar una red contra amenazas internas es una prioridad más baja porque los empleados de la empresa representan un riesgo de seguridad bajo.
- [x] Tanto los piratas informáticos con experiencia que son capaces de escribir su propio código de fallas como aquellas personas sin experiencia que descargan fallas de Internet representan una amenaza grave para la seguridad de la red.
- [ ] Suponiendo que una empresa ubica su servidor Web afuera del firewall y tiene copias de seguridad adecuadas del servidor Web, no se necesitan más medidas de seguridad para proteger el servidor Web, ya que la intrusión de un pirata informático no puede provocar perjuicio alguno.
- [ ] Los sistemas operativos de red establecidos como UNIX y los protocolos de red como TCP/IP se pueden utilizar con su configuración predeterminada, ya que no presentan debilidades de seguridad inherentes.
- [x] Proteger los dispositivos de red contra el daño físico provocado por el agua o la electricidad es una parte necesaria de la política de seguridad.

12 La convención de nombres de la imagen de Cisco IOS permite la identificación de diferente versiones y capacidades del IOS. ¿Qué información se puede reunir del nombre de archivo **c2600-d-mz.121-4**?

(Elija dos opciones).

- [ ] El "mz" en el nombre de archivo representa las capacidades especiales y funciones del IOS.
- [ ] El archivo no está comprimido y requiere 2.6 MB de RAM para ejecutarse.
- [x] El software es versión 12.1, cuarta revisión.
- [ ] El archivo se descarga y tiene 121.4MB de tamaño.
- [x] El IOS es para la plataforma de hardware serie Cisco 2600.

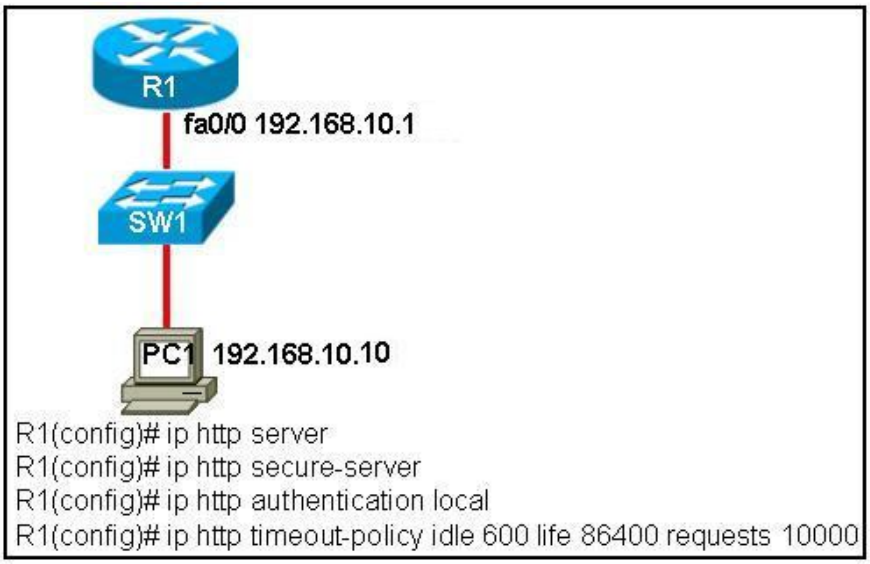
13 ¿Cuáles de las siguientes son dos afirmaciones verdaderas con respecto a evitar ataques a la red? (Elija dos opciones).

- [ ] Es posible confiar en la seguridad de la configuración de seguridad predeterminada de los servidores y sistemas operativos para PC modernos.
- [ ] Los sistemas de prevención de intrusión pueden registrar actividades de red sospechosas, pero no existe una manera de contrarrestar un ataque en curso sin la intervención del usuario.
- [x] La mitigación de las amenazas a la seguridad física consiste en controlar el acceso a los puertos de consola del dispositivo, rotular los tendidos de cable críticos, instalar sistemas UPS y proporcionar control ante condiciones climáticas.
- [ ] La mejor forma de evitar ataques de suplantación de identidad es utilizar dispositivos firewall.
- [x] Cambiar contraseñas y nombres de usuario predeterminados y desactivar o desinstalar los servicios innecesarios son aspectos del endurecimiento de los dispositivos.

14 ¿Cuáles de las siguientes son dos condiciones que el administrador de red debe verificar antes de intentar actualizar una imagen del IOS de Cisco mediante un servidor TFTP? (Elija dos opciones).

- [ ] Verificar el nombre del servidor TFTP mediante el comando **show hosts**.
- [ ] Verificar que el servidor TFTP se esté ejecutando mediante el comando **tftpdnld**.
- [ ] Verificar que la check sum de la imagen sea válida, mediante el comando **show version**.
- [x] Verificar la conectividad entre el router y el servidor TFTP mediante el comando **ping**.
- [x] Verificar que haya suficiente memoria flash para la nueva imagen del IOS de Cisco mediante el comando **show flash**.

15



Consulte la ilustración. El administrador de dispositivos de seguridad (SDM, Security Device Manager) está instalado en el router R1. ¿Cuál es el resultado de abrir un explorador Web en la PC1 e introducir la URL **https://192.168.10.1**?

- ( ) La contraseña se envía en forma de texto sin cifrar.
- ( ) Se establece una sesión Telnet con R1.
- (•) La página del SDM de R1 aparece con un cuadro de diálogo que solicita un nombre de usuario y contraseña.
- ( ) Se muestra la página de inicio de R1 y permite que el usuario descargue los archivos de configuración e imágenes de IOS de Cisco.

Sistema de evaluación

Saltar a Tiempo restante | Saltar a Navegación | Saltar a Temas de la evaluación

ComputingPeru

Comenzar la evaluación - EWAN Chapter 4 - CCNA Exploration: Acceso a la WAN (Versión 4.0)

Tiempo restante: 00:38:55

Mostrando 2 de 2 Siguiente> Página: 2 IR <Ant.

16

```
<resultado omitido>
!
username sdm privilege 5 password 0 sdm
!
ip http server
ip http authentication local
ip http secure-server
ip http timeout-policy idle 600 life 86400 requests 10000
!
<resultado omitido>
!
line con 0
line aux 0
line vty 0 4
 privilege level 15
 login local
 transport input telnet ssh
```

Consulte la ilustración. Un administrador de red está intentando configurar un router para que use SDM, pero no está funcionando correctamente. ¿Cuál podría ser el problema?

- (•) El nivel de privilegio del usuario no está configurado correctamente.
- ( ) El método de autenticación no está correctamente configurado.
- ( ) El servidor HTTP no está correctamente configurado.
- ( ) La política de tiempo de espera de HTTP no está correctamente configurada.

17 ¿Qué dos afirmaciones son verdaderas acerca de los ataques de red? (Elija dos opciones).

- [ ] Las contraseñas seguras de red mitigan la mayoría de los ataques DoS.
- [ ] Los gusanos requieren de la interacción humana para propagarse, no así los virus.
- [ ] Los ataques de reconocimiento siempre son de naturaleza electrónica, como barridos de ping o escaneos de puertos.
- [x] Un ataque de fuerza bruta busca cada contraseña posible a través de una combinación de caracteres.
- [x] Los dispositivos internos no deben confiar plenamente en los dispositivos de la DMZ y la comunicación entre la DMZ y los dispositivos internos debe ser autenticada para impedir ataques como la reorientación de los puertos.

18 ¿Qué paso se requiere para recuperar una contraseña de enable de un router que se haya perdido?

- (•) Establezca el registro de configuración para eludir la configuración de inicio.
- ( ) Copie la configuración en ejecución en la configuración de inicio
- ( ) Vuelva a cargar el IOS desde un servidor TFTP desde ROMMON.
- ( ) Vuelva a configurar el router a través del modo Setup

19 ¿Cuál es la mejor defensa para proteger una red ante vulnerabilidades de suplantación de identidad?

- ( ) Programar escaneos de antivirus.
- ( ) Programar escaneos de antispyware.
- (•) Programar capacitación para los usuarios.
- ( ) Programar actualizaciones del sistema operativo.

20 El director de TI comenzó una campaña para recordar a los usuarios que no deben abrir mensajes de correo electrónico de origen sospechoso. ¿Contra qué tipo de ataques está intentando proteger a

los usuarios el director de TI?

- DoS
- DDoS
- virus
- acceso
- reconocimiento

21

```
R3# show running-config
<resultado omitido>
interface serial0/0/0
ip ospf  message-digest-key 1 md5 cisco
<resultado omitido>
```

Consulte la ilustración. ¿Cuál es el objetivo de la afirmación "**ip ospf message-digest-key 1 md5 cisco**" en la configuración?

- Especificar una clave que se utiliza para autenticar actualizaciones de enrutamiento.
- Guardar ancho de banda comprimiendo el tráfico.
- Habilitar la encriptación de SSH del tráfico.
- Crear un túnel de IPsec.

22 ¿Cuáles de los siguientes son dos objetivos que debe lograr una política de seguridad? (Elija dos opciones).

- [ ] proporcionar una lista de verificación de instalación de los servidores seguros
- [ ] describir la manera en la que se debe configurar el firewall
- [x] documentar los recursos que se deben proteger
- [x] Identificar los objetivos de seguridad de la organización
- [ ] identificar las tareas específicas que supone el endurecimiento de un router