

16.4.6 Sara Rocío Miranda Mateos 0244643

0244643@up.edu.mx

Cisco Packet Tracer - /Users/saramiranda/Downloads/16.4.6-packet-tracer---configure-secure-passwords-and-ssh_es-XL.pka - Sara Rocío Miranda Mateos - 2023-07-11 21:09:36

Activity Results

Time Elapsed: 00:35:00

Congratulations Sara Rocío Miranda Mateos! You completed the activity.

Overall FeedbackAssessment ItemsConnectivity Tests

Expand/Collapse AllShow Incorrect Items

Assessment Items	Status	Points	Component(s)	Feedback
Network				
PCA				
Default Gateway	Correct	10	Default Gateway...	
Ports				
FastEthernet0				
IP Address	Correct	8	IPv4 Host Addr...	
Subnet Mask	Correct	2	IPv4 Host Addr...	
RTA				
DNS				
IP Domain-Lookup	Correct	0	Other	
Enable Secret	Correct	1	Configuration M...	
Host Name	Correct	5	Basic Security C...	
IP Domain Name	Correct	5	Hostname Confi...	
Login Options				
Blocking				
Attempts	Correct	2	Device Hardenin...	
Duration	Correct	2	Device Hardenin...	
Enabled	Correct	4	Device Hardenin...	
Period	Correct	2	Device Hardenin...	
Ports				
GigabitEthernet0/0				
IP Address	Correct	8	Device Interface ...	
Port Status	Correct	4	Device Interface ...	
Subnet Mask	Correct	8	Device Interface ...	
Security				
Modulus Bits	Correct	0	Other	
Security Password Min-Length	Correct	10	Device Hardenin...	
Service Password Encryption	Correct	1	Basic Security C...	
Startup Config	Correct	5	Basic Security C...	
User Names	Correct	5	Configuration M...	
(deprecated) Username	Correct	0	Other	
VTY Lines				
VTY Line 0				

Score: 213/213

Item Count: 67/67

Component	Items/Total	Score
Basic Security Configuration	9/9	33/33
Configuration Management	4/4	12/12
Default Gateway Configuration	2/2	15/15
Device Hardening Configuration	42/42	93/93
Device Interface Configuration	6/6	40/40
Hostname Configuration	2/2	10/10
IPv4 Host Address Configuration	2/2	10/10

Close

Packet Tracer - Configure contraseñas seguras y SSH

Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
RTA	G0/0	172.16.1.1	255.255.255.0	N/D
PCA	NIC	172.16.1.10	255.255.255.0	172.16.1.1
SW1	VLAN 1	172.16.1.2	255.255.255.0	172.16.1.1

Situación

El administrador de red le ha pedido que prepare **RTA** y **SW1** para la implementación. Antes de que puedan conectarse a la red, se deben habilitar las medidas de seguridad.

Instrucciones

Paso 1: Configure la seguridad básica en el enrutador

a. Configure el direccionamiento IP en **PCA** de acuerdo con la tabla de direccionamiento.

b. Consola en RTA desde la Terminal en PCA.

c. Configure el nombre de host como **RTA**.

d. Configure el direccionamiento IP en **RTA** y habilite la interfaz.

e. Cifre todas las contraseñas no cifradas.

```
RTA(config)# service password-encryption
```

f. Establezca la longitud mínima de la contraseña en 10.

```
RTA(config)# security password min-length 10
```

g. Establezca la contraseña secreta segura que desee. **Nota:** Elija una contraseña que recuerde, o tendrá que restablecer la actividad si está bloqueado fuera del dispositivo.

h. Desactive la búsqueda de DNS.

```
RTA(config)# no ip domain-lookup
```

i. Establezca el nombre de dominio en **CCNA.com** (distingue entre mayúsculas y minúsculas para la puntuación en PT).

```
RTA(config)# ip domain-name CCNA.com
```

j. Cree un usuario de su elección con una contraseña cifrada segura.

```
RTA(config)# username any_user secret any_password
```

k. Genere claves RSA de 1024bits.

Nota: En Packet Tracer, ingrese la clave criptográfica generar el comando `rsa` y presione Entrar para continuar.

```
RTA(config)# crypto key generate rsa
```

El nombre de las claves será: **RTA.CCNA.com**

Elija el tamaño del módulo clave en el rango de 360 a 2048 para sus llaves de uso general. Elegir un módulo clave mayor que 512 puede tomar unos minutos.

How many bits in the modulus [512]: **1024**

- I. Bloquee durante tres minutos a cualquier persona que no pueda iniciar sesión después de cuatro intentos en un período de dos minutos.

```
RTA(config)# login block-for 180 attempts 4 within 120
```

- m. Configure todas las líneas VTY para el acceso SSH y use los perfiles de usuario locales para la autenticación.

```
RTA (config) # línea vty 0 4
RTA(config-line)# transport input ssh
RTA(config-line)# login local
```

- n. Establezca el tiempo de espera del modo EXEC en 6 minutos en las líneas VTY.

```
RTA(config-line)# exec-timeout 6
```

- o. Guarde la configuración en la NVRAM.

- p. Acceda al símbolo del sistema en el escritorio de **PCA** para establecer una conexión SSH a **RTA**.

```
C:\ > ssh/?
Packet Tracer PC SSH
Uso: SSH -l username target
C:\ >
```

Paso 2: Configure la seguridad básica en el Switch

Configure el conmutador **SW1** con las medidas de seguridad correspondientes. Consulte los pasos de configuración del router si necesita ayuda adicional.

- a. Haga clic en **SW1** y seleccione la pestaña **CLI**.
- b. Configure el nombre de host como **SW1**.
- c. Configure el direccionamiento IP en SW1 **VLAN1** y habilite la interfaz.
- d. Configure la dirección de gateway predeterminado.
- e. Deshabilite todos los puertos de conmutador no utilizados.

Nota: En un switch, es una buena práctica de seguridad deshabilitar los puertos no utilizados. Un método para hacer esto es simplemente apagar cada puerto con el comando **'shutdown'**. Esto requeriría acceder a cada puerto individualmente. Existe un método de acceso directo para realizar modificaciones en varios puertos a la vez mediante el **comando** **interface range**. En **SW1**, todos los puertos excepto FastEthernet0/1 y GigabitEthernet0/1 se pueden apagar con el siguiente comando:

```
SW1 (config) # interface range F0/2-24, G0/2
SW1 (config-if-range) # shutdown
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
<Output omitted>
%LINK-5-CAMBIADO: Interfaz FastEthernet0/24, cambié el estado a administrativamente inactivo
```

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down

El comando utilizó el rango de puertos de 2-24 para los puertos FastEthernet y, a continuación, un rango de puertos único de GigabitEthernet0/2.

- f. Cifre todas las contraseñas de texto.
- g. Establezca la contraseña secreta segura que desee.
- h. Desactive la búsqueda de DNS.
- i. Establezca el nombre de dominio en **CCNA.com** (distingue entre mayúsculas y minúsculas para la puntuación en PT).
- j. Cree un usuario de su elección con una contraseña cifrada segura.
- k. Genere claves RSA de 1024 bits.
- l. Configure todas las líneas VTY para el acceso SSH y use los perfiles de usuario locales para la autenticación.
- m. Establezca el tiempo de espera del modo EXEC en 6 minutos en todas las líneas VTY.
- n. Guarde la configuración en la NVRAM.