Configurazione delle password per le porte Telnet, console e AUX nei router

Sommario

Introduzione

Questo documento fornisce esempi di configurazione della password di protezione per le connessioni EXEC in ingresso al router.

Prerequisiti

Requisiti

Per eseguire le attività descritte in questo documento, è necessario disporre di un accesso in modalità di esecuzione privilegiata all'interfaccia della riga di comando (CLI) del router. Per informazioni sull'utilizzo della riga di comando e sulle modalità di comando, vedere Utilizzo dell'interfaccia della riga di comando di Cisco IOS.

Per istruzioni sul collegamento di una console al router, consultare la documentazione fornita con il router oppure la documentazione in linea dell'apparecchiatura.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Router Cisco 2509
- Software Cisco IOS® versione 12.2(19)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

L'utilizzo della protezione con password per controllare o limitare l'accesso all'interfaccia della riga di comando (CLI) del router è uno degli elementi fondamentali di un piano di sicurezza generale.

La protezione del router dall'accesso remoto non autorizzato, in genere Telnet, è la protezione più comune che deve essere configurata, ma non può essere ignorata.

Nota: la protezione tramite password è solo una delle numerose operazioni da eseguire in un sistema di sicurezza di rete avanzato ed efficace. I firewall, gli elenchi degli accessi e il controllo dell'accesso fisico alle apparecchiature sono altri elementi da prendere in considerazione quando si implementa il piano di sicurezza.

La riga di comando, o EXEC, consente di accedere a un router in diversi modi, ma in tutti i casi la connessione in entrata al router è effettuata su una riga TTY. Esistono quattro tipi principali di linee TTY, come mostrato in questo esempio di **visualizzazione** dell'output di **linea**:

```
2509#show line
   Tty Typ     Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns   Int
*    0 CTY               -    -      -    -    -      0       0     0/0       -
     1 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     2 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     3 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     4 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     5 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     6 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     7 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     8 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     9 AUX   9600/9600   -    -      -    -    -      0       0     0/0       -
    10 VTY               -    -      -    -    -      0       0     0/0       -
    11 VTY               -    -      -    -    -      0       0     0/0       -
    12 VTY               -    -      -    -    -      0       0     0/0       -
    13 VTY               -    -      -    -    -      0       0     0/0       -
    14 VTY               -    -      -    -    -      0       0     0/0       -

2509#
```

Il tipo di linea **CTY** è la porta console. Su qualsiasi router, viene visualizzato nella configurazione del router come **riga con 0** e nell'output del comando **show line** come **città**. La porta console viene utilizzata principalmente per l'accesso al sistema locale tramite un terminale console.

Le linee **TTY** sono linee asincrone utilizzate per le connessioni del modem in entrata o in uscita e le connessioni del terminale e possono essere visualizzate in una configurazione di router o server di accesso come **linea x**. I numeri di riga specifici sono una funzione dell'hardware incorporato o installato sul router o sul server di accesso.

La linea **AUX** è la porta ausiliaria, visualizzata nella configurazione come **linea AUX 0**.

Le linee **VTY** sono le linee terminali virtuali del router, usate solo per controllare le connessioni Telnet in entrata. Sono virtuali, nel senso che sono una funzione del software - non c'è hardware associato ad essi. Nella configurazione vengono visualizzati come **riga vty 0 4**.

Ciascuno di questi tipi di linea può essere configurato con una password di protezione. Le righe possono essere configurate in modo da utilizzare una sola password per tutti gli utenti o per password specifiche dell'utente. Le password specifiche dell'utente possono essere configurate localmente sul router oppure è possibile utilizzare un server di autenticazione per fornire l'autenticazione.

Non è vietato configurare linee diverse con diversi tipi di password di protezione. Infatti, è comune vedere i router con una sola password per la console e password specifiche dell'utente per altre connessioni in entrata.

Di seguito è riportato un esempio di output del router restituito dal comando **show running-config**:

```
2509#show running-config
Building configuration...

Current configuration : 655 bytes
!
version 12.2
.
.
.
!--- Configuration edited for brevity line con 0 line 1 8 line aux 0 line vty 0 4 ! end
```

Configura password sulla riga

Per specificare una password su una riga, utilizzare il comando **password** in modalità di configurazione riga. Per abilitare il controllo della password all'accesso, usare il comando **login** in modalità di configurazione riga.

Procedura di configurazione

In questo esempio, viene configurata una password per tutti gli utenti che tentano di utilizzare la console.

1. Dal prompt di EXEC privilegiato (o "enable"), accedere alla modalità di configurazione e quindi passare alla modalità di configurazione della linea utilizzando i comandi seguenti. Il prompt viene modificato in base alla modalità corrente.
   ```
   router#configure terminal
   ```

```
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#line con 0
router(config-line)#
```

2. Configurare la password e abilitare il controllo della password all'accesso.
```
router(config-line)#password letmein
router(config-line)#login
```

3. Uscire dalla modalità di configurazione.
```
router(config-line)#end
router#
%SYS-5-CONFIG_I: Configured from console by console
```
Nota: non salvare le modifiche alla configurazione **sulla riga con 0** finché non viene verificata la possibilità di accedere.

Nota: nella configurazione della console della linea, **login** è un comando di configurazione obbligatorio per abilitare il controllo della password all'accesso. L'autenticazione da console richiede sia la **password** che i comandi di **accesso** per funzionare.

Verifica della configurazione

Esaminare la configurazione del router per verificare che i comandi siano stati immessi correttamente:

- **show running-config**: visualizza la configurazione corrente del router.
```
router#show running-config
Building configuration...
...
!--- Lines omitted for brevity ! line con 0 password letmein
login
line 1 8
line aux 0
line vty 0 4
!
end
```
Per verificare la configurazione, disconnettersi dalla console ed eseguire nuovamente l'accesso utilizzando la password configurata per accedere al router:
```
router#exit

router con0 is now available

Press RETURN to get started.

User Access Verification
Password:
!--- Password entered here is not displayed by the router router>
```
Nota: prima di eseguire il test, verificare di disporre di una connessione alternativa al router, ad esempio Telnet o dial-in, in caso di problemi durante il login al router.

Risoluzione dei problemi di accesso non riuscito

se non è possibile accedere nuovamente al router e la configurazione non è stata salvata, il ricaricamento del router eliminerà le modifiche apportate alla configurazione.

Se le modifiche alla configurazione sono state salvate e non è possibile accedere al router, sarà necessario eseguire un recupero della password. Per istruzioni sulla piattaforma in uso, vedere Procedure di recupero della password.

Configura password locali specifiche dell'utente

Per stabilire un sistema di autenticazione basato sul nome utente, utilizzare il comando **username** in modalità di configurazione globale. Per abilitare il controllo della password all'accesso, utilizzare il comando **login local** in modalità di configurazione riga.

Procedura di configurazione

Nell'esempio, le password sono configurate per gli utenti che tentano di connettersi al router sulle linee VTY con Telnet.

1. Dal prompt dei comandi in modalità di esecuzione privilegiata (o "abilitazione"), accedere alla modalità di configurazione e immettere le combinazioni nome utente/password, una per ciascun utente per il quale si desidera consentire l'accesso al router:
   ```
   router#configure terminal
   Enter configuration commands, one per line.  End with CNTL/Z.
   router(config)#username russ password montecito
   router(config)#username cindy password belgium
   router(config)#username mike password rottweiler
   ```

2. Passare alla modalità di configurazione riga utilizzando i comandi seguenti. Il prompt viene modificato in base alla modalità corrente.
   ```
   router(config)#line vty 0 4
   router(config-line)#
   ```
3. Configurare il controllo della password all'accesso.
   ```
   router(config-line)#login local
   ```

4. Uscire dalla modalità di configurazione.
   ```
   router(config-line)#end
   router#
   %SYS-5-CONFIG_I: Configured from console by console
   ```
   Nota: per disabilitare la funzione Auto Telnet quando si digita un nome sulla CLI, **non** configurare una **registrazione preferita** sulla linea in uso. Mentre il comando **transport preferred none** restituisce lo stesso output, la funzione auto Telnet viene disabilitata per l'host definito e configurato con il comando **ip host**. A differenza del comando **no logging preferred**, che interrompe l'accesso per gli host non definiti e lo permette di utilizzare quelli definiti.

Verifica della configurazione

Esaminare la configurazione del router per verificare che i comandi siano stati immessi correttamente:

- **show running-config**: visualizza la configurazione corrente del router.
  ```
  router#show running-config
  Building configuration...
  !
  !--- Lines omitted for brevity ! username russ password 0 montecito
  username cindy password 0 belgium
  username mike password 0 rottweiler
  !
  !--- Lines omitted for brevity ! line con 0 line 1 8 line aux 0 line vty 0 4 login local
  !
  ```

```
end
```

Per verificare questa configurazione, è necessario connettersi al router in modalità Telnet. A tale scopo, è possibile connettersi da un host diverso della rete, ma è possibile anche eseguire il test dal router stesso effettuando una connessione via telnet all'indirizzo IP di qualsiasi interfaccia del router in stato attivo/attivo, come mostrato nell'output del comando **show interfaces**.Di seguito è riportato un esempio di output se l'indirizzo dell'**interfaccia ethernet 0** è 10.1.1.1:

```
router#telnet 10.1.1.1
Trying 10.1.1.1 ... Open


User Access Verification


Username: mike
Password:
!--- Password entered here is not displayed by the router router
```

Risoluzione dei problemi relativi alla password specifica dell'utente

I nomi utente e le password distinguono tra maiuscole e minuscole. Gli utenti che tentano di eseguire l'accesso con un nome utente o una password errati verranno rifiutati.

Se gli utenti non sono in grado di accedere al router con le loro password specifiche, riconfigurare il nome utente e la password sul router.

Configura password riga AUX

Per specificare una password sulla riga AUX, usare il comando **password** in modalità di configurazione riga. Per abilitare il controllo della password all'accesso, usare il comando **login** in modalità di configurazione riga.

Procedura di configurazione

Nell'esempio, viene configurata una password per tutti gli utenti che tentano di utilizzare la porta AUX.

1. Usare il comando **show line** per verificare la linea usata dalla porta AUX.

```
R1#show line

   Tty Typ     Tx/Rx    A Modem Roty AccO AccI  Uses  Noise  Overruns  Int
*    0 CTY                   -    -     -    -     -     0      0     0/0       -
    65 AUX  9600/9600    -    -     -    -    -     0     1     0/0             -
    66 VTY                  -    -     -    -    -     0      0     0/0       -
    67 VTY                  -    -     -    -    -     0      0     0/0       -
```

2. Nell'esempio, la porta AUX è sulla linea 65. Utilizzare questi comandi per configurare la linea AUX del router:

```
R1# conf t
R1(config)# line 65
R1(config-line)#modem inout
R1(config-line)#speed 115200
R1(config-line)#transport input all
R1(config-line)#flowcontrol hardware
```

```
R1(config-line)#login
R1(config-line)#password cisco
R1(config-line)#end
R1#
```

Verifica configurazione

Esaminare la configurazione del router per verificare che i comandi siano stati immessi correttamente:

- Il comando **show running-config** visualizza la configurazione corrente del router:

```
R1#show running-config
Building configuration...
!
!--- Lines omitted for brevity. line aux 0
 password cisco
 login
 modem InOut
 transport input all
 speed 115200
 flowcontrol hardware

!--- Lines omitted for brevity. ! end
```

Configurazione dell'autenticazione AAA per l'accesso

Per abilitare l'autenticazione di autenticazione, autorizzazione e accounting (AAA) per gli account di accesso, utilizzare il comando **login authentication** in modalità di configurazione riga. È necessario configurare anche i servizi AAA.

Procedura di configurazione

Nell'esempio, il router è configurato in modo da recuperare le password degli utenti da un server TACACS+ quando gli utenti tentano di connettersi al router.

Nota: la configurazione del router per l'utilizzo di altri tipi di server AAA (ad esempio, RADIUS) è simile. Per ulteriori informazioni, vedere Configurazione dell'autenticazione.

Nota: questo documento non prende in considerazione la configurazione del server AAA.

1. Dal prompt dei comandi in modalità di esecuzione privilegiata (o "abilitazione"), accedere alla modalità di configurazione e immettere i comandi per configurare il router in modo che utilizzi i servizi AAA per l'autenticazione:

```
router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#aaa new-model
router(config)#aaa authentication login my-auth-list tacacs+
router(config)#tacacs-server host 192.168.1.101
router(config)#tacacs-server key letmein
```

2. Passare alla modalità di configurazione riga utilizzando i comandi seguenti. Il prompt viene modificato in base alla modalità corrente.

```
router(config)#line 1 8
router(config-line)#
```

3. Configurare il controllo della password all'accesso.
```
router(config-line)#login authentication my-auth-list
```

4. Uscire dalla modalità di configurazione.
```
router(config-line)#end
router#
%SYS-5-CONFIG_I: Configured from console by console
```

Verifica della configurazione

Esaminare la configurazione del router per verificare che i comandi siano stati immessi correttamente:

- **show running-config**: visualizza la configurazione corrente del router.

```
router#write terminal
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router
!
aaa new-model
aaa authentication login my-auth-list tacacs+
!
!--- Lines omitted for brevity ... ! tacacs-server host 192.168.1.101
tacacs-server key letmein
!
line con 0
line 1 8
 login authentication my-auth-list
line aux 0
line vty 0 4
!
end
```

Per provare questa particolare configurazione, è necessario effettuare una connessione in entrata o in uscita alla linea. Per informazioni specifiche sulla configurazione delle linee asincrone per le connessioni modem, consultare la Guida alla connessione modem - router.

In alternativa, è possibile configurare una o più linee VTY per eseguire l'autenticazione AAA ed eseguire i relativi test.

Risoluzione dei problemi di accesso AAA

Prima di usare i comandi **debug**, consultare le informazioni importanti sui comandi di debug.

Per risolvere un problema relativo a un tentativo di accesso non riuscito, utilizzare il comando **debug** appropriato alla configurazione:

- debug autenticazione aaa
- raggio di debug
- debug kerberos

Informazioni correlate

- Guida di riferimento ai comandi di Cisco IOS Debug
- Supporto tecnico – Cisco Systems