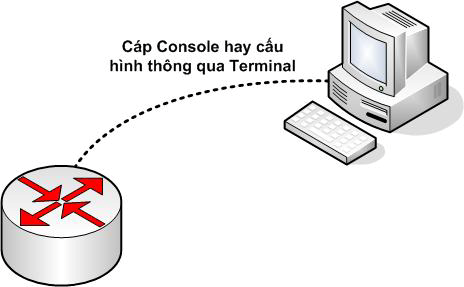
**LAB 13: KHÔI PHỤC MẬT KHẨU CHO CISCO**

**ROUTER**

**I. Giới thiệu :**

- Mật khẩu truy cập là rất hữu ích trong lĩnh v ực bảo mật, tuy nhiên đôi khi nó cũng đem l ại phiền toái nếu chẳng may bạn quên mất mật khẩu truy nhập.Bài thực hành khôi phục mật khẩu cho Cisco Router này giúp bạn khôi phục lại mật khẩu để đăng nhập vào Router .

**Lưu ý** : Đặt mật khẩu cho Router có ý nghĩa r ất lớn trong khía cạnh security,nó ngăn cản được các phiên **Telnet** từ xa vào Router để thay đổi cấu hình hay thực hiện những mục đích khác.Bạn nên tránh nhầm lẫn giữa hai khái niệm “bảo mật” và “khôi phục mật khẩu”,bạn có thể khôi phục hay thay đổi được mật khẩu của Router không có nghĩa là mức độ bảo mật của Router không cao vì để khôi phục mật khẩu cho Router, **điều kiện tiên quyết** là bạn phải **thao tác trực tiếp trên Router**, điều này có nghĩa là b ạn phải được sự chấp nhận của Admin hay kỹ thuật viên quản lý Router.



**II. Mô tả bài lab và đồ hình :**

Trong đồ hình trên PC nối với router bằng cáp *console*

**III. Quá trình khởi động của Router :**

Khi vừa bật nguồn, Router sẽ kiểm tra phần cứng, sau khi phần cứng đã được kiểm tra hoàn tất, hệ điều hành sẽ được nạp từ Flash, tiếp đó Router sẽ nạp cấu hình trong NVRAM bao gồm tất cả những nội dung đã cấu hình trước cho Router như các thông tin về giao thức, địa chỉ các cổng và cả mật khẩu truy nhập.Vì vậy để Router không kiểm tra mật khẩu khi đăng nhập, bạn phải ngăn không cho Router nạp dữ liệu từ NVRAM.

Mỗi dòng Router có một kỹ thuật khôi phục mật khẩu khác nhau, tuy vậy để khôi phục mật khẩu cho Router bạn phải qua các bước sau:

 *Bước 1* : Khới động Router,ngăn không cho Router nạp cấu hình trong NVRAM. (bằng

cách thay đổi thanh ghi từ 0x2102 sang thanh ghi 0x2142).

 *Bước 2* : Reset lại Router (lúc này Router sử dụng thanh 0x2142 để khởi động).

 *Bước 3* : Đăng nhập vào Router(lúc này Router không kiểm tra mật khẩu), dùng các lệnh của Router để xem hay cài đặt lại mật khẩu (bạn chỉ xem được mật khẩu khi mật khẩu được cài đặt ở chế độ không mã hóa)

 *Bước 4* : Thay đổi thanh ghi (từ 0x2142 sang 0x2102).

 *Bước 5* : Lưu lại cấu hình vừa cài đặt (lúc này mật khẩu đã biết).

**IV. Khôi phục mật khẩu cho Cisco Router 2500.**

- Giả sử khi bạn đăng nhập vào Router nhưng bạn quên mất mật khẩu.

TTG con0 is now available Press RETURN to get started. TTG>enable

Password: Password: Password:

% Bad secrets

- Bạn phải thực hiện việc khôi phục mật khẩu. Các bước thực hiện như sau:

 **Bước 1** : bạn khởi động lại Router

System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE

Copyright (c) 1986-1995 by cisco Systems

2500 processor with 8192 Kbytes of main memory← *ấn* **Ctrl Break** *không cho*

*Router nạp dữ liệu từ NVRAM*

Abort at 0x103AA7E (PC)

romon> **confreg 0x2142**← *Sử dụng lệnh này để thay đổi thanh ghi sang* **0x2142**

 **Bước 2** : khởi động lại Router, lúc này Router sẽ nạp cấu hình từ thanh ghi 0x2142 (cấu hình trắng)

TTG>enable ← *password sẽ không yêu cầu kiểm tra khi đăng nhập*

TTG#show start ← *dùng lệnh Show start xem cấu hình trong NVRAM*

Using 456 out of 32762 bytes

!

version 12.1

no service single-slot-reload-enable service timestamps debug uptime service timestamps log uptime

no service password-encryption

!

hostname Router

!

enable secret 5 $1$AqeQ$yB00zFjHxIiVoHLnbLEhh1 ← *password secret đã*

*được mã hoá*

enable password cisco ← *mật khẩu enable password là cisco*

!

end

 **Bước 3** : Cấu hình lại mật khẩu cho Router: TTG#configure terminal

Enter configuration commands, one per line. End with CNTL/Z. TTG(config)#enable secret TTG ← *mật khẩu secret được cấu hình lại là TTG* TTG(config)#exit

TTG#conf igure terminal

TTG(config)#enable password **class** ← *mật khẩu enable password là class*

TTG(config)#exit

 **Bước 4** : Thay đổi thanh ghi hiện hành từ **0x2142** trở về **0x2102**

Dùng lệnh **Show version** để xem thanh ghi hiện hành

**TTG#show verion**

Cisco Internetwork Operating System Software

IOS (tm) 2500 Software (C2500-I-L), Version 12.1(26), RELEASE SOFTWARE (fc1) Copyright (c) 1986-2004 by cisco Systems, Inc.

Compiled Sat 16-Oct-04 02:44 by cmong

Image text-base: 0x03042000, data-base: 0x00001000

2 Serial network interface(s)

32K bytes of non-volatile configuration memory.

16384K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2142 ← *Thanh ghi* ***0x2142*** *đang được sử dụng*

 **Thay đổi thanh ghi:**

TTG(config)#config-register 0x2102 ← *dùng lệnh* ***config-register***

TTG(config)#exit

 **Xem lại thanh ghi hiện hành: TTG#show version**

Cisco Internetwork Operating System Software

IOS (tm) 2500 Software (C2500-I-L), Version 12.1(26), RELEASE SOFTWARE (fc1) Copyright (c) 1986-2004 by cisco Systems, Inc.

Compiled Sat 16-Oct-04 02:44 by cmong

2 Serial network interface(s)

32K bytes of non-volatile configuration memory.

16384K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2142 (will be 0x2102 at next reload) ← *thanh ghi hiện hành là* ***0x2102***

 **Bước 5** : lưu cấu hình đã thay đổi vào thanh ghi 0x2102

**TTG#copy run start** Building configuration... [OK]

- Dùng lệnh **show start** để xem cấu hình khởi động trong NVRAM TTG#show start

Using 488 out of 32762 bytes

!

version 12.1

no service single-slot-reload-enable service timestamps debug uptime service timestamps log uptime

no service password-encryption

!

hostname TTG

!

enable secret 5 $1$49cD$jrvYyRSQhpTAHuDA1/R1v. enable password class

!

!

! End

- Sau khi **reload** lại, đăng nhập vào Router,mật khẩu **secret** là **TTG** sẽ được kiểm tra

TTG con0 is now available Press RETURN to get started. TTG>ena

Password: ← *mật khẩu là TTG sẽ đươc kiểm tra và chấp nhận*

TTG#

**V. Phụ lục các lệnh liên quan đến bài lab :**

|  |  |
| --- | --- |
| Router #**show version** | Khi bạn sử dụng câu lệnh show version  thì dòng cuối cùng của phần hiển thị sẽ thông báo cho bạn biết giá trị của Configuration register. |
| Router (config)#**config-register 0x2102** | Thay đổi giá trị của Configuration  Register thành 2102 |
| Rommon 1 > **confreg 0x2142** | Thay đổi giá trị thanh ghi trong chế độ  Rommon thành 2142 |
| Router #**reload** | Khởi động lại Router |
| Router #**copy runningconfig startup-**  **config** | Copy file cấu hình vào NVRAM |

128

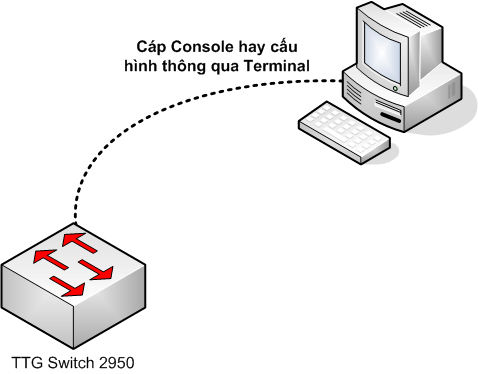
**Lab 14: RECOVERY PASSWORD SWITCH**

**I. Giới thiệu :**

Trong bài lab này chúng ta se thực hiện recovery password của một switch

**II. Mô tả bài lab và đồ hình :**

- Nối cáp console giữa PC với switch. Chúng ta sẽ tiến hành recovery password trên switch 2950 trong bài lab này.



**III. Thực hiện :**

- Để khảo sát việc recovery password rõ ràng ơhn ,chúng ta s ẽ cấu hình tên và password cho

switch trước khi tiến hành recovery password cho switch

- Chúng ta cấu hình tên và password cho switch như sau : Switch#configure terminal Switch(config)#hostname TTG

TTG(config)#enable password cisco *← Đặt password cho switch*

TTG(config)#enable secret TTG *← Đặt secret password cho switch*

- Sau khi cấu hình xong chúng ta lưu vào NVRAM và xem lại cấu hình trong NVRAM đó trư ớc khi tiến hành recovery password cho switch.

TTG#copy run start

Destination filename [startup-config]? Building configuration...

TTG#show start

TTG#sh start

Using 1186 out of 32768 bytes version 12.1

***hostname TTG***

***enable secret 5 $1$s22D$vCe6IFIeKLhUPZqgm6QZ6/***

***enable password cisco***

Chúng ta tiến hành recovery password theo cách bước sau :

 **Bước 1** : tắt nguồn switch, sau đó giữa nút MODE trên switch 2950 trong lúc bật nguồn lại. Khi màn hình hiện những thông báo sau, ta nhả nút MODE ra.

Cisco Internetwork Operating System Software

IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA2, RELEASE SOFTWARE (fc1)

Copyright (c) 1986-2004 by cisco Systems, Inc. Compiled Sun 07-Nov-04 23:14 by antonino

… (*một số thông báo được lược bỏ*) …

**flash\_init load\_helper boot**

 **Bước 2**: Chúng ta nhập ***flash\_init*** đễ bắt đầu cấu hình cho các file của flash. Nhập câu lệnh ***dir flash:*** để xem các file có chứa trong flash. Sau đó chúng ta đổi tên file config.text thành config.bak (vì cấu hình của chúng ta đã lưu ph ần trước được switch chứa trong file này) bằng câu lệnh sau : ***rename flash:config.text flash:config.bak*** Sau đó chúng ta reload lại switch bằng câu lệnh ***boot***

 **Bước 3** : Trong quá trình khởi động switch sẽ hỏi : Continue with the configuration dialog? [yes/no] :

Chúng ta nhập vào ***NO***, để bỏ qua cấu hình này. Sau khi khởi động xong chúng ta vào mode privileged.

Switch>en

Switch#

- Sau đó chúng ta chuyển tên file config.bak trong flash thành config.text bằng cách : Switch#rename flash:config.bak flash:config.text

- Rồi cấu hình NVRam vào RAM bằng câu lệnh sau : Switch#copy flash:config.text system:running-config

 **Bước 4** : gở bỏ tất cả các loại password

TTG#conf t

TTG(config)#no enable password

TTG(config)#no enable secret

 **Bước 5 :** copy cấu hình từ RAM vào NVRam, rồi reload switch lại.

TTG#copy run start

Destination filename [startup-config]? ↵

Building configuration... [OK]

TTG#reload

**IV. Phụ lục một số lệnh liên quan đến bài lab :**

|  |  |
| --- | --- |
| Switch: **flash\_init** | Khởi tạo bộ nhớ flash |
| Switch: **dir flash:** | Hiển thị nội dung của bộ nhớ flash |
| Switch: **rename flash:config.text**  **flash:config.bak** | Thực hiện đổi tên của file cấu hình. Vì file  cấu hình config.text có chứa mật khẩu. |
| switch: **boot** | Khởi động lại switch |
| Switch #**rename flash:config.bak**  **flash:config.text** | Đổi lại tên của file cấu hình trở về tên  mặc định. |
| Switch #**copy flash:config.text**  **system:running-config** | Copy file cấu hình trong bộ nhớ flash |

Switch#**copy running-config startupconfig**

Lưu file cấu hình đang chạy vào NVRAM

với mật khẩu mới đã được cấu hình.