บทที่ 3

Lab Password Recovery

นาย ประสิทธ์ บุญประเสริฐ (Mr-boy) เรียบเรียง

Password Recovery คือการกู้ Password

สำหรับผู้ที่ใช้งาน Router cisco อยู่เกิดพบปัญหาว่าลืมรหัสผ่านต่าง ๆ ในการ Hack เข้ามาใช้งานยังตัว Router โดยตรง เช่น ลืมรหัสผ่านสำหรับ Port console (Password Line Console) หรือลืมรหัสผ่านของตัว enable secret หรือ enable password ซึ่งเป็นรหัสผ่านก่อนเข้าสู่การใช้งาน ในโหมด Admin หรือที่นิยมเรียกกันทั่วไปคือโหมดenable ถ้าลืมแล้วจะทำอย่างไร วิธีการที่นิยมใช้ทำกัน ก็คือ การทำ "Password recovery"นั่นเองและการทำงานต้อง Console ทำที่หน้าเครื่องเท่านั้น

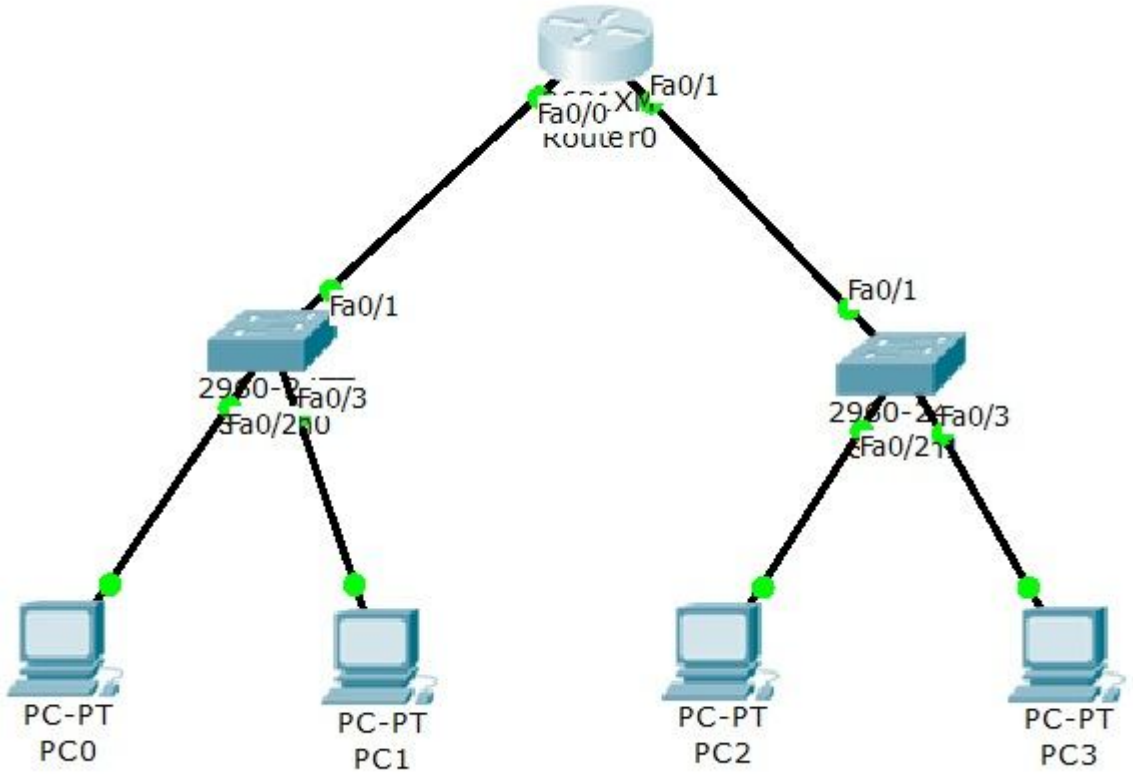
Lab 1. ให้ทำการ Recovery Password ของ Router

Password Recovery มี 9 ขั้นตอนดังนี้

Here are the main steps to password recovery:

1. Boot the router and interrupt the boot sequence by performing a break, which will take the router into ROM monitor mode.
2. Change the configuration register to turn on bit 6 (with the value 0x2142).
3. Reload the router.
4. Enter privileged mode.
5. Copy the startup-config file to running-config.
6. Change the password.
7. Reset the configuration register to the default value.
8. Save the router configuration.
9. Reload the router (optional).

ให้วาดภาพดังนี้ หรือ Load Lab Basic Config



User Access Verification

Password:

jodoi>en

Password:

Password:

Password:

% Bad secrets

ทดสอบเข้า Router จะติด password ไม่สามารถเข้าไป Config ได้

เฉลย LAB Password Recovery

ก่อนจะทำการ Recovery จะต้องทำความรู้จักกับค่า Configuration register ก่อน ค่า Configuration register หรือ ค่า bootstrap คือ ค่าที่ใช้กำหนดว่าจะให้ Router cisco ไป เรียกค่า Config จากที่ใด (nvram หรือ ram)จะเป็นเลขบิต โดยค่าDefaultของ Router ทุกตัว คือ 0x2102 สามารถใช้ Command show version เพื่อดูค่านี้ได้ โดยข้อความจะแสดงอยู่บรรทัดล้างสุดว่า

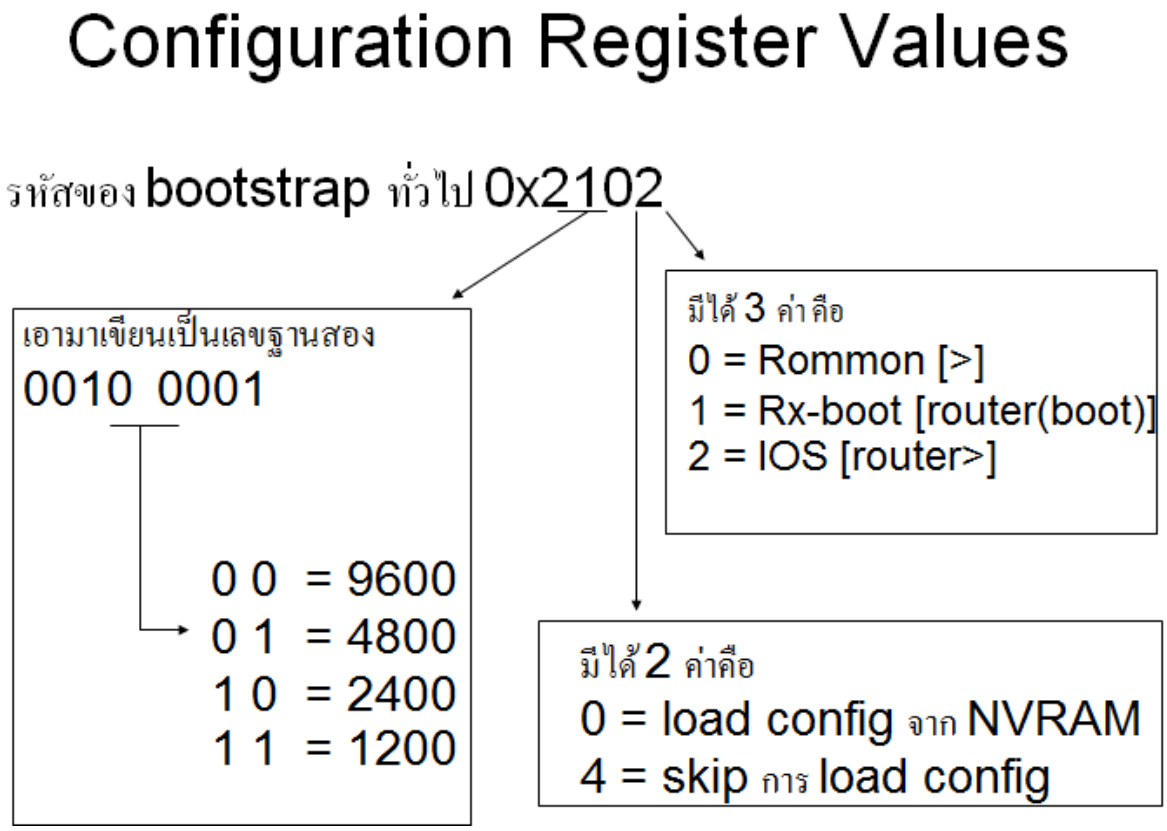
Configuration register is 0x2102

0x ที่นำหน้า 2102 นั้นหมายความว่า ตัวเลขที่อยู่หลัง 0x เป็นเลขฐาน 16 ให้ดูบิตที่ 6 จะเป็น

การกำหนดว่าจะให้ Router Boot จากอะไรที่แนะนำคือเลข 0,4 โดย

เลข 0 เป็นการกำหนดให้ Router โหลด Config จาก nvram หรือ startup

เลข 4เป็นการข้ามการโหลด Config ที่ nvram



ซึ่งการ Recovery Password ต้องเข้ามากำหนดค่า จาก 0x2102 เป็น 0x2142 เพื่อข้าม

ขั้นตอนการโหลดConfig จาก nvram ให้ได้

สรุปขั้นตอนในการทำPassword Recovery มีอยู่ 9 ขั้นตอน

1. Reboot Router ใหม่ ด้วยการปิดเปิดสวิตช์ในขณะที่ Router กำลังBootให้ขัดจังหวะการBoot ด้วยการ

กดปุ่ม Ctrl+Break หรือ Ctrl+C จะขึ้นคำว่าrommon 1 > ดังรูปภาพ

```
System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
cisco 2621 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory


Self decompressing the image :
########################
monitor: command "boot" aborted due to user interrupt
rommon 1 >
```

Command ที่ใช้

2. เปลี่ยนค่า Configuration registerให้เป็นค่า 0x2142

3. reload ใหม่

4. เข้าสู่โหมด enable หรือ Privileged mode

5. ดึงค่า config เดิมที่อยู่ใน nvramหรือ startupมาไว้ที่ ram หรือ running copy startup-config running-config

6. ทำการแก้ไขรหัสผ่านต่าง ๆ

7. เปลี่ยนค่า Configuration registerให้กลับมาเป็นค่า Default (0x2102)

8. ทำการ save config ที่แก้ไขเสร็จแล้วcopy running-config startup-config

9. reload ใหม่

ตัวอย่างขั้นตอนการทำงานพร้อมคำสั่งที่ใช้งาน ในการRecovery Password

กรณีลืมรหัสผ่านคอนโซล (Line Console) จะเห็นว่าเราไม่สามารถเข้ามาใช้ Router ได้

1. ทำการปิดเปิด Router และในขณะ Router กำลัง Boot ให้ กด Ctrl + Break เพื่อเข้าสู่โหมด Rommon

2. เปลี่ยนค่า Configuration register ให้เป็น 0x2142 โดยใช้ คำสั่ง confreg 0x2142

3. reload ใหม่ ด้วยคำสั่งboot หรือ reset

หลังจาก Router บูตขึ้นมาใหม่ Router ไม่ได้อ่านค่า comfig จาก nvram จาก Register number ที่เรา กำหนดไว้ จะเห็นได้ว่า เราเข้า Router ได้โดยไม่ติด Password จาก Command Prompt ที่ถามว่าต้องการ setup ค่าต่างๆ ให้ตอบ NO

4.เข้าสู่โหมด enable หรือ Privileged EXEC เพื่อเข้าไปแก้ไขค่า config ต่าง ๆ ด้วยคำสั่ง enable

5.ดึงค่า Conifg เดิมที่อยู่ใน nvram หรือ startup มาไว้ที่ ram หรือ running เพื่อทำการแก้ไข โดยใช้ คำสั่งว่า copy startup-config running-config

ก่อนทำการดึง Config กลับมาให้ทำการ

show startup-config เพื่อดูค่า Config ที่เราทำการเซฟไว้ใน nvram

จะเห็นค่า Config เดิมที่ทำการเซฟไว้ล่าสุด จะเห็นว่ามีการตั้งhostname , enable password, enable secret ไว้ และทำการ # show running-configเพื่อดูค่า Config ปัจจุบัน หรือค่า Defaultเทียบกันดู และทำการดึงไฟล์ Config เดิมกลับมาโดยใช้คำสั่ง# copy startup-config running-config

จะเห็นว่าเมื่อดึงค่า Config เดิมกลับมาแล้ว Hostnameจะเปลี่ยน เนื่องจากที่ startup มีการตั้งชื่อ Hostnameไว้ ให้ทำการ show startup-config และ show running-config เทียบกันดูจะเห็นว่าค่า Config ทั้งสองส่วนเหมือนกันแล้ว

6. แก้ไขรหัสผ่านต่างๆ ดังนี้ยกตัวอย่าง..

ต้องการเปลี่ยน Password Line Console

jodoi(config) # line console 0

jodoi(config-line) # password 1234

jodoi(config-line) # login

เปลี่ยนรหัสผ่าน enable passwordให้เป็น cisco

jodoi(config) # enable password cisco

กรณีนี้ ที่ต้องการลบ enable secret

jodoi(config) # no enable secret

7.เปลี่ยนค่า Configuration registerให้กลับมาเป็นค่า Default (0x2102) โดยใช้คำสั่ง

config-register ตามด้วยค่า register number ที่ต้องการเปลี่ยน คือ 0x210

jodoi(config) # config-register 0x2102

8. Save Config ที่ทำการแก้ไขมาทั้งหมด ด้วยคำสั่งcopy running-config startup-config

jodoi # copy running-config startup-config

9. Reload Router ใหม่ ในโหมดของ Router ปกติ ให้ใช้คำสั่งreload

jodoi # reload

หลังจาก Reload Router ใหม่แล้ว จะต้องเข้า Router ได้ด้วย รหัสผ่านที่เราแก้ไข

หวังว่าบทความนี้ จะก่อประโยชน์สำหรับผู้ที่ทำงานอยู่กับอุปกรณ์ Cisco ไม่มากก็น้อยนะครับ

สนับสนุนโดย http://www.jodoi.com

Pasit_boy@jodoi.com