# BEBERAPA KONFIGURASI KEAMANAN PADA ROUTER CISCO

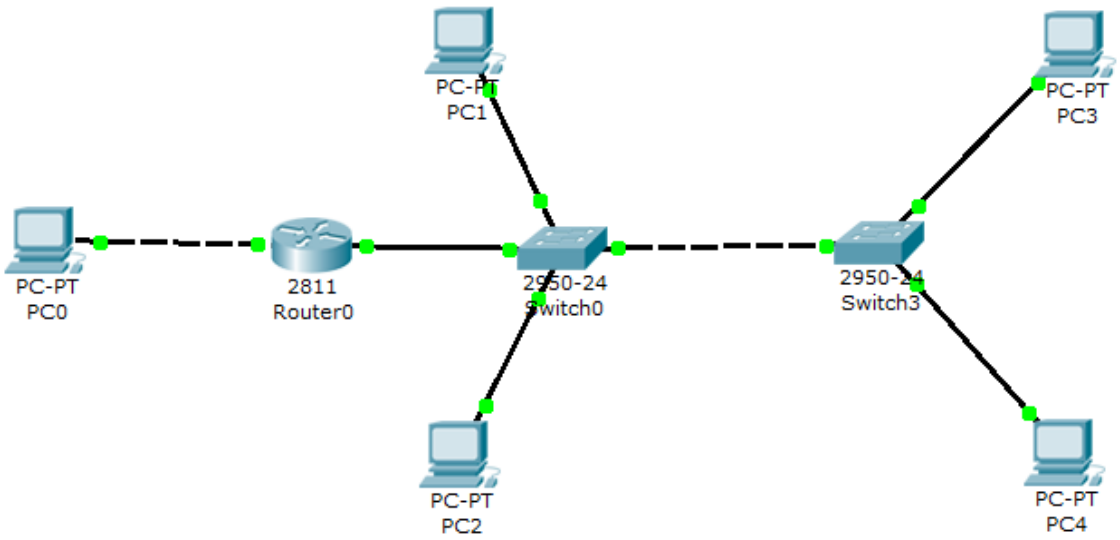
**Firman Setya Nugraha**

*Someexperience.blogspot.com*

*Firmansetyan@gmail.com*



Dalam bidang IT, keamanan jaringan sangatlah dibutuhkan karena hal tersebut menyangkut data pentingyang sifatnya rahasia, baik bagi personal maupun enterprise. Kali ini saya akan mencoba membahas tentang konfigurasi keamanan pada Router Cisco.



1. Keamanan pada console
   Keamanan pada console berfungsi untuk mencegah agar oarang lain tidak bisa sembarangan mengakses router dengan kabel rollover.

   Router >enable

   Router #conf t

   Router(config) # int fa0/0

   Router(config-if) # ip add 192.168.0.1 255.255.255.0

   Router(config-if) #no shut

   Router(config-if) # exit

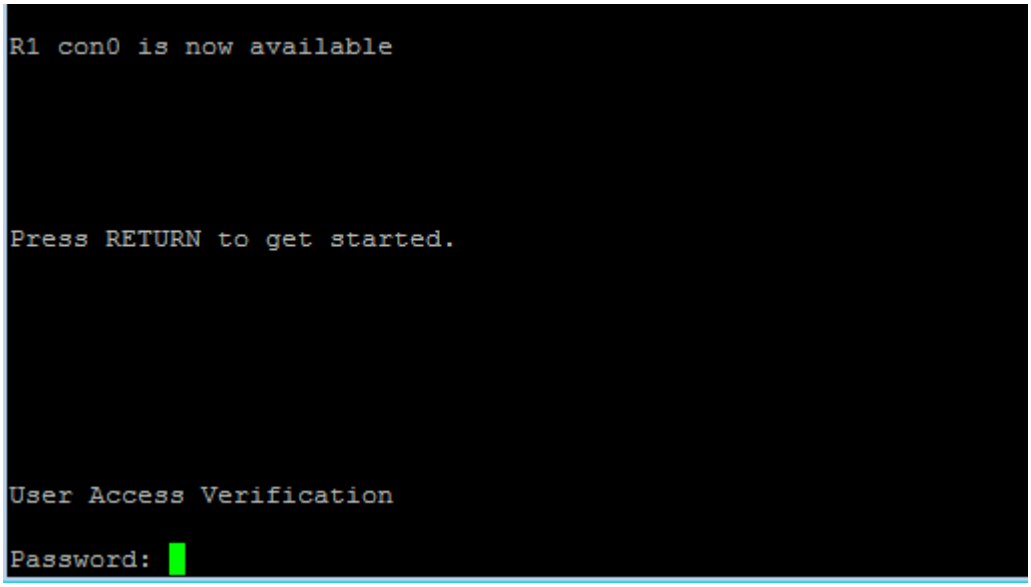
   Router(config) #line con 0

   Router(config-line) #password cisco

   Router(config-line) #login

   Router(config-line) #end

   Maka ketika kita akan mengakses router akan ada tampilan seperti dibawah ini:




   Sehingga kita tidak akan bisa mengakses router lewat console tanpa menggunakan password “cisco”.

1. Keamanan remote
   Keamanan remote membatasi seseorang mengakses lewat remote, dengan menggunakan telnet atau SSH.

   Router >enable

   Router #conf t

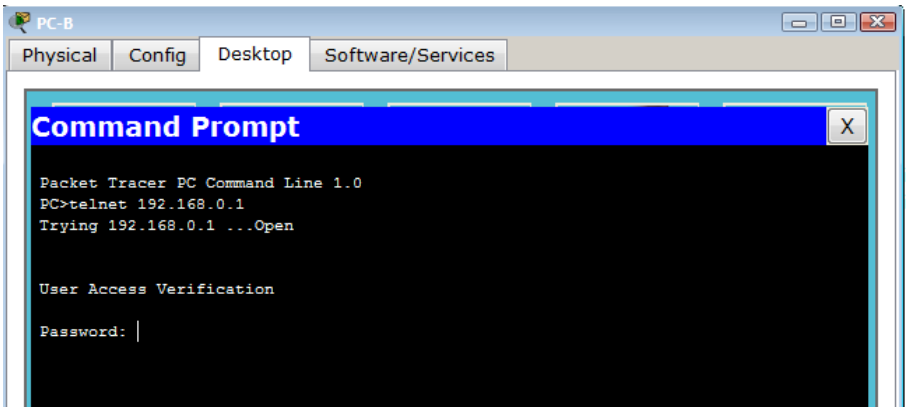
   Router(config) #line vty 0 4

Router(config-if) # password router

Router(config-if) # login

Router(config-if) # end

Maka ketika kita akan masuk lewat telnet maupun SSH akan dimintai password:



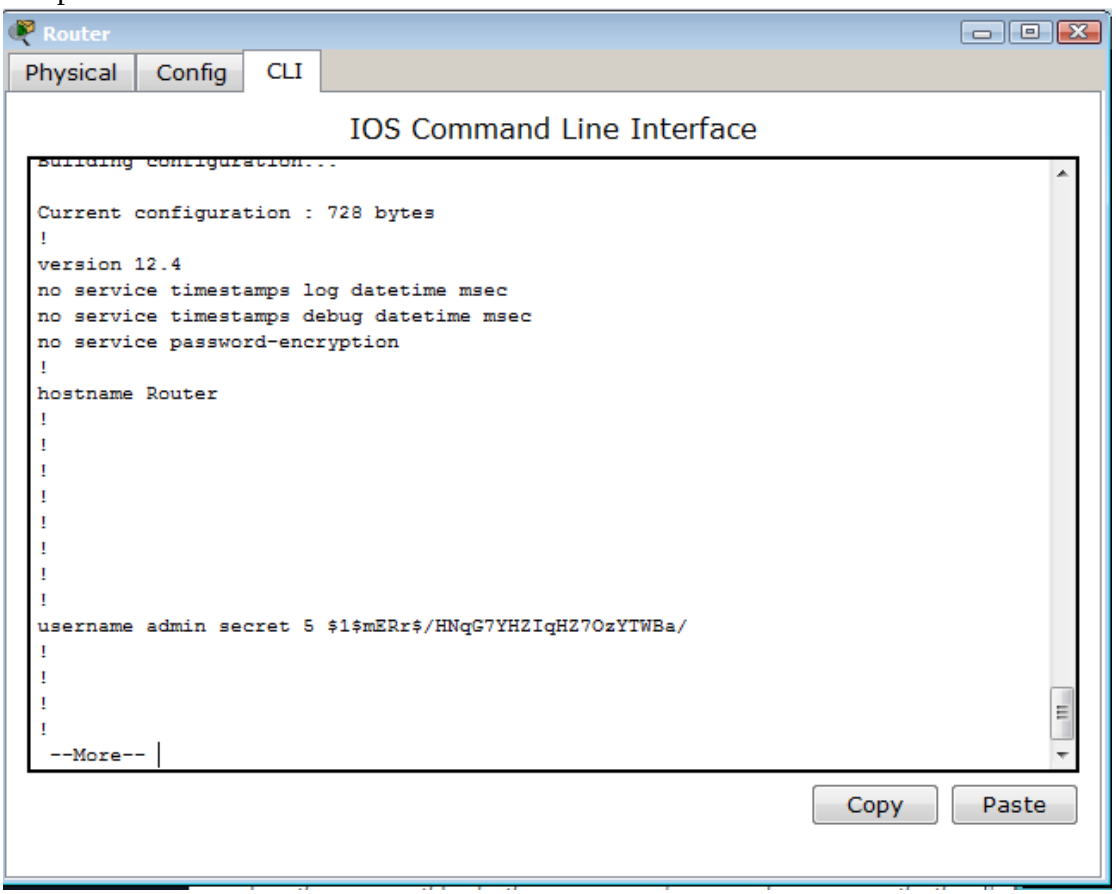

2. Keamanan previlege user
   Keamanan previleged user digunakan sebagi security sebelum masuk ke provileged user mode. Ada beberapa keamanan previleged mode:
   a. Router(config)# **enable password** *password*
      Digunakan untuk menetapkan password baru atau mengubah kata sandi yang ada untuk tingkat previleged command. Akan tetapi **enable password** tingkat enkripsinya kurang dan hanya digunakan apabila Cisco IOS software yang digunakan sudah tua. Dan password dapat terlihat apabila mengetikkan perintah show run
   b. Router(config)# enable password [level level] {password| encryption-type encrypted-password}

      atau

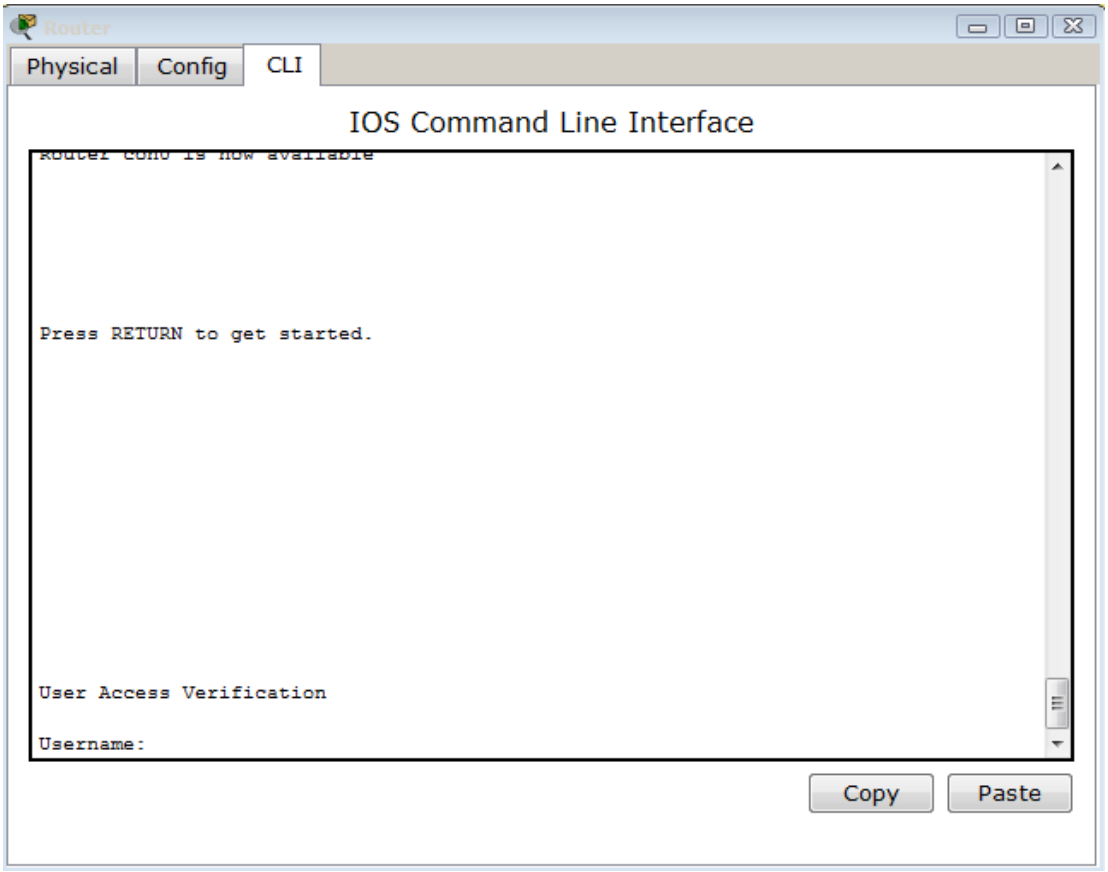
      Router(config)# enable secret [level level] {password | encryption-type encrypted-password}
      Digunakan untuk menentukan password untuk tingkat perlakuan tertentu. Setelah menentukan tingkat dan menetapkan password, memberikan password hanya untuk pengguna yang membutuhkan akses pada tingkat tertentu. Kelebihannya adalah ketika mengetik show run pada privilege user mode, password sudah dienkripsi

3. Memberi hak akses username
   Router(config)# username admin secret indonesia
   *NB: password pada console 0 harus dihapus sehingga pada show run terlihat bahwa console memiliki tipe login local. Apabila ketika di show run hanya terdapat keterangan login, dapat dirumah menjadi login local, sehingga ketika masuk akan dimintai username dan password.

Biasanya digunakan untuk Radius server sehingga tercatat username yang mengakses router tersebut. Ketika keluat dan akan masuk akan diminta memasukkan username dan password




Gambar ketika mengetikkan sh run

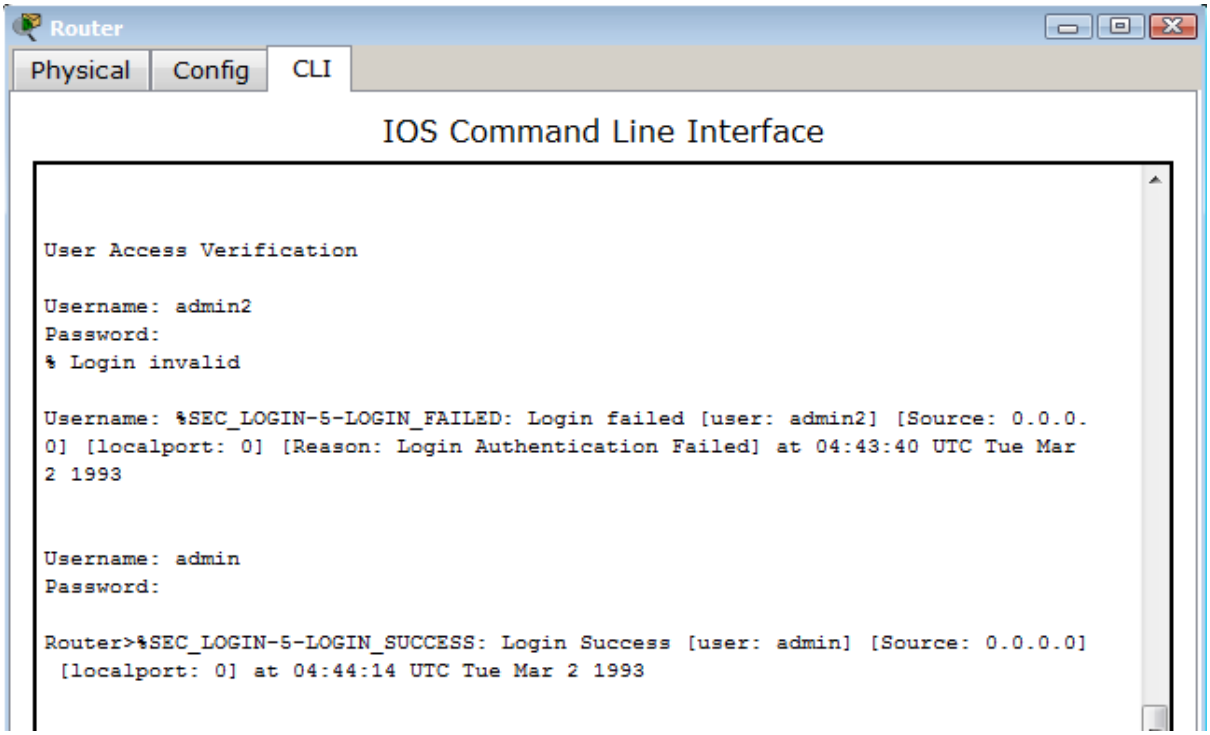



Gambar setelah pemberian password pada username

Untuk membatasi security passowd, dapat digunakan perintah:
Router(config)#security passwords min-length 8
Hal diatas mempunyai maksud bahwa password yang dibuat haruslah 8 karakter atau lebih.

Untuk membuat catatan siapa saja yang masuk dapat digunakan perintah:
Router(config) #login on-failure log
Router(config) #login on-success log
Router(config) #exit

Sehingga ketika gagal atau berhasl akan ada tampilan catatan seperti gambar dibawah ini:




Selanjutnya kita juga dapat membatasi waktu blokir apabila ada yang mencoba masuk dan gagal dengan perintah:
Router(config) # login block-for 5400 attempts 3 with 180
Maksudnya adalah apabila mencoba login 3kali dan gagal dalam 180 detik, maka akses ke router akan diblokir 5400detik atau setara 1,5 jam.

Mengatur time out remote dan console dengan perintah:

- Time out remote
  Router(config) # line vty 0 4
  Router(config-line) # exex-timeout 3
  Router(config-line) # exit
  Maksudnya adalah time out untuk masuk ke global configuration mode selama 3 menit
- Time out console
  Router(config) # line console 0
  Router(config-line) # exex-timeout 2
  Router(config-line) # exit
  Maksudnya adalah time out untuk masuk ke global configuration mode selama 2 menit

4. Mengenkripsi keseluruhan password

   Router >enable

   Router #conf t

   Router(config) # service password-encryption

Router(config) # exit

Password encrypton digunakan pada seluruh password, meliputi authentikasi key password, previleged command password, console dan virtual terminal line access password, dan BGP neighbor password. Jadi berguna untuk menenkripsi sehingga semua password telah terenkripsi di file konfigurasi.

5. Identifikasi port

   Router(config) # ip identd

   Digunakan untuk support identifikasi sehngga memungkinkan permintaan Transmission Control Protocol (TCP) port untuk identifikasi (untuk melaporkan identitas klien memulai koneksi TCP dan sejumlah menanggapi koneksi.). Fitur ini memungkinkan protokol aman. Dengan dukungan identifikasi, Dapat menghubungkan port TCP pada host, mengeluarkan string teks sederhana untuk meminta informasi, dan menerima balasan text-string sederhana.

Jenis-jenis previleged:

Secara umum ada 3 previlege levels pada router

1. Privilege level 1= non-previleged (promt is outer>), default level untuk logging in.
2. Privilege level 15=privileged (promt is rotuer#), level seterlah enable mode
3. Privilege level 0=jarang digunakan, tetapi mencakup 5 perintah: disable, enable, exit, help, dan logout

Level 2-14 tidak dipakai dalam default configuration tetapi perintah normalnya level 15 dapat dipindahkan ke salah satu dari level tersebut dan perintah level 1 dapat pindak ke salah satu dari level tersebut. Sehingga kemanan ini tergantung pengaturan administrasi pada router.

Referensi:


- http://zweimesserschmitt.wordpress.com/2012/10/24/konfigurasi-keamanan-dasar-pada-router-cisco-2/
- https://zweimesserschmitt.wordpress.com/2012/10/21/konfigurasi-keamanan-dasar-pada-router-cisco-1/
- http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a008009465c.shtml
- http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfpass.html#wp1001357