Pentesting Attack Router Reconstructed Cracking cisco-ios password

BY

Vishal Shah

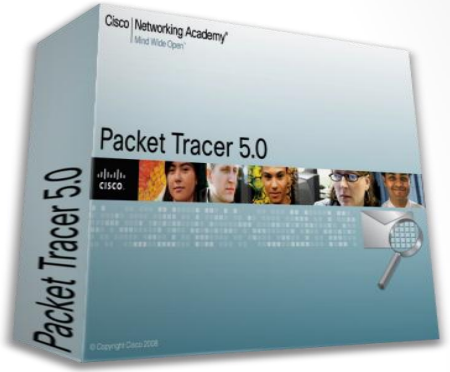
Hackcept.blogspot.com

Thanks to Neo ,Silent poison ,Silicon, Inxroot

vishalshah731@gmail.com

Setup and tools Requirement for breaking cisco password

- Download and install Cain & Abel from http://www.oxid.it/cain.htm

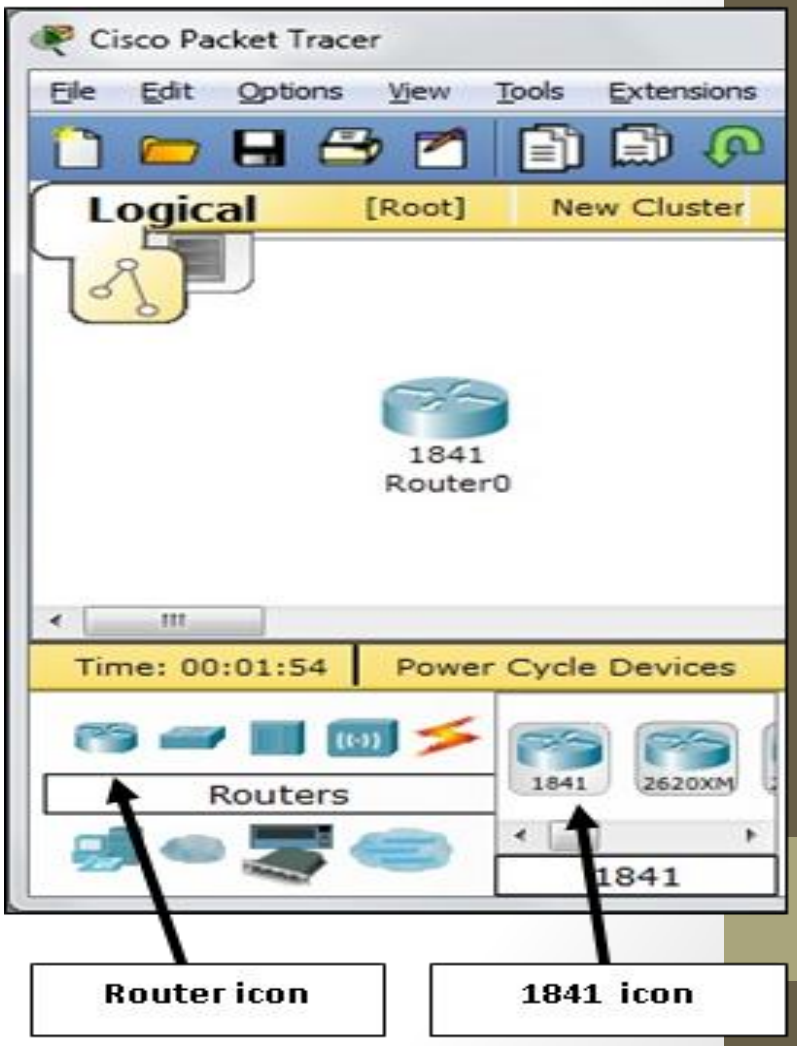


- Packet Tracer, the Cisco router

simulator installed in windows http://www.packettracer.info/

Working Steps:

- Install Packet Tracer with the default options.
- Launch Packet Tracer.
- In the lower left corner of the “Cisco Packet Tracer” window, click the Router icon, as shown to the right on this page.
- In the lower center of the “Cisco Packet Tracer” window, drag the 1841 icon into the white center pane, as shown to the right on this page.



Adding Password To The Router

- Double click on center of the “Cisco Packet Tracer” window, double-click the "**1841 Router 0**" icon.

- In the "Router0" window, click the **CLI** tab, as shown in the figure on the next page. At the "**Continue with configuration dialog? [yes/no]**" prompt, press **n** and then press **Enter** key twice.

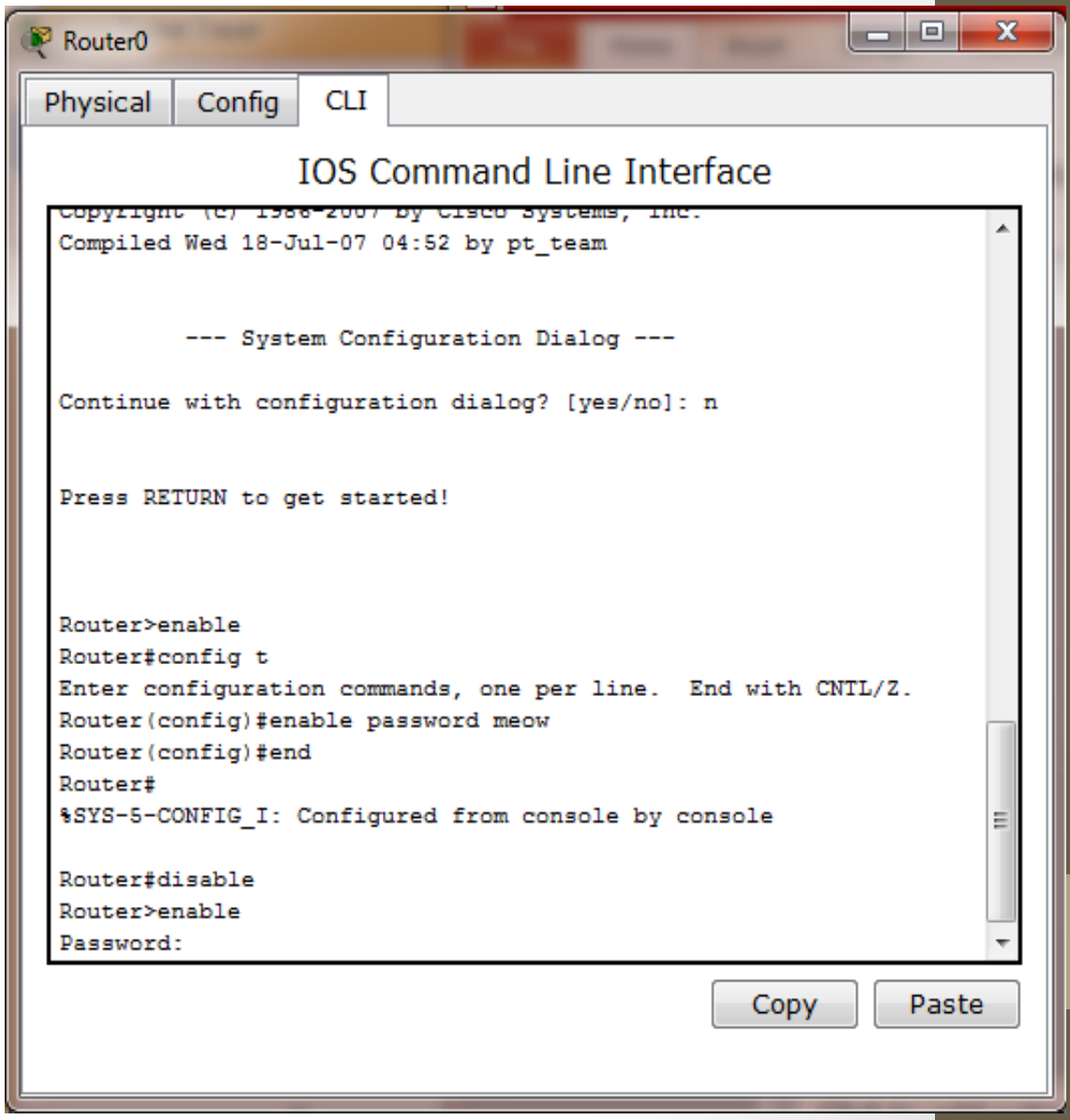
- You should see a **Router>** prompt. This is the Cisco IOS, which is a lot like Linux. The **>** indicates that you are in **Unprivileged Mode**, like a non-administrative account. To enter Privileged mode, type this command, and then press the Enter key:
  enable

- The prompt changes to **Router#**. You are now in **Privileged Mode**, like root on a Linux computer. You didn't need a password to elevate your privileges, which is very insecure. To fix that, you must first enter **Global Configuration Mode**. Type this command, and then press the Enter key:
  config t

- The prompt changes to **Router(config)#**. To require a password of **cisco**, type this command, and then press the Enter key:
  enable password meow

Screenshot - Setting Up Password In Cisco router

- To exit Global Configuration Mode, type this command, and then press the Enter key:
  End
- To exit Privileged Mode, type this command, and then press the Enter key:
  enable password meow
- To exit Global Configuration Mode, type this command, and then press the Enter key:
  end
- To exit Privileged Mode, type this command, and then press the Enter key:
  disable



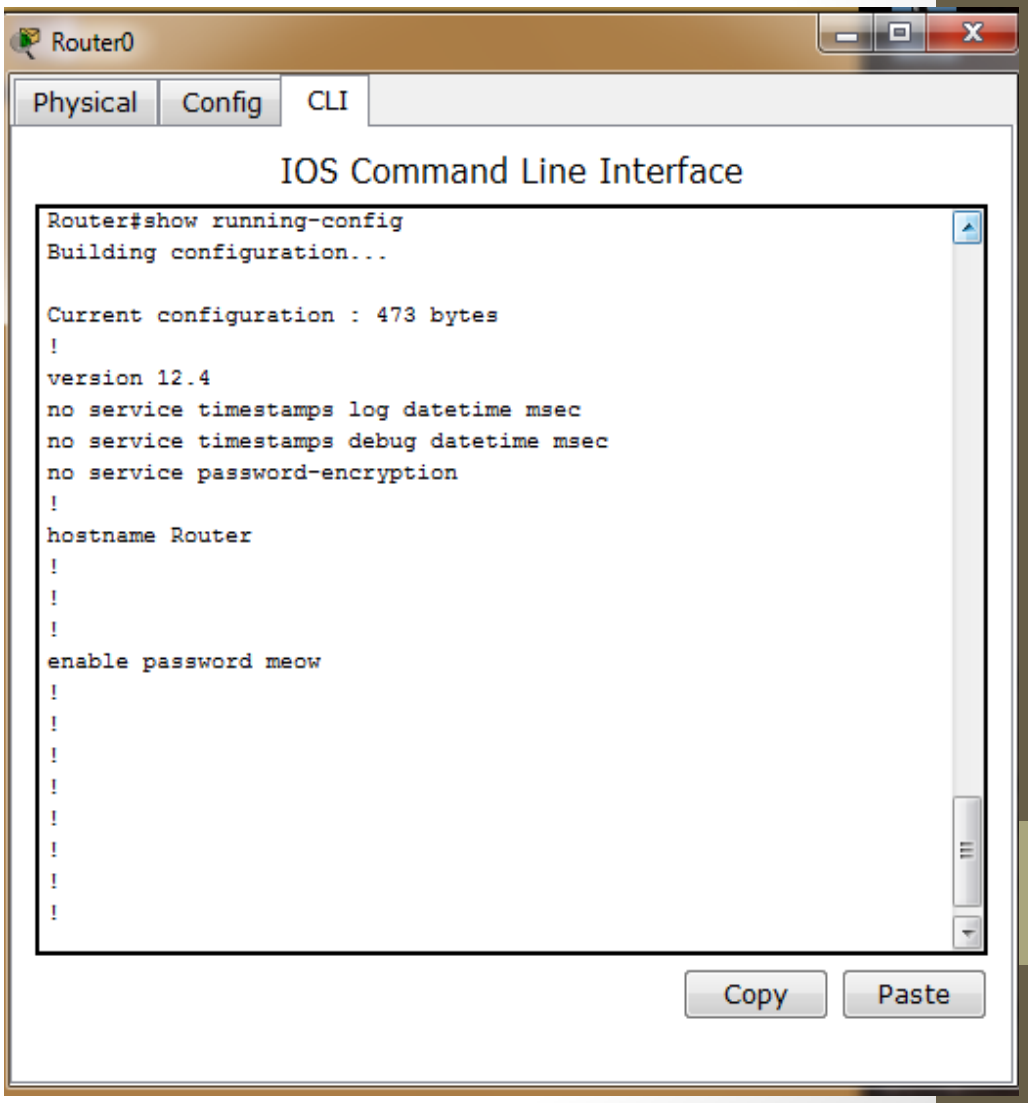
Looking The Configuration File and Removing Plain Text Password

- The router is now password-protected, but how secure is the password storage? To find out, type this command, and then press the Enter key:
  show running-config

- The password is clearly visible, as shown to the right on this page.

Removing the Plaintext Password
Plaintext storage of passwords is very insecure. To remove that stored password, type these commands, pressing the Enter key after each command:

config t
no enable password
end



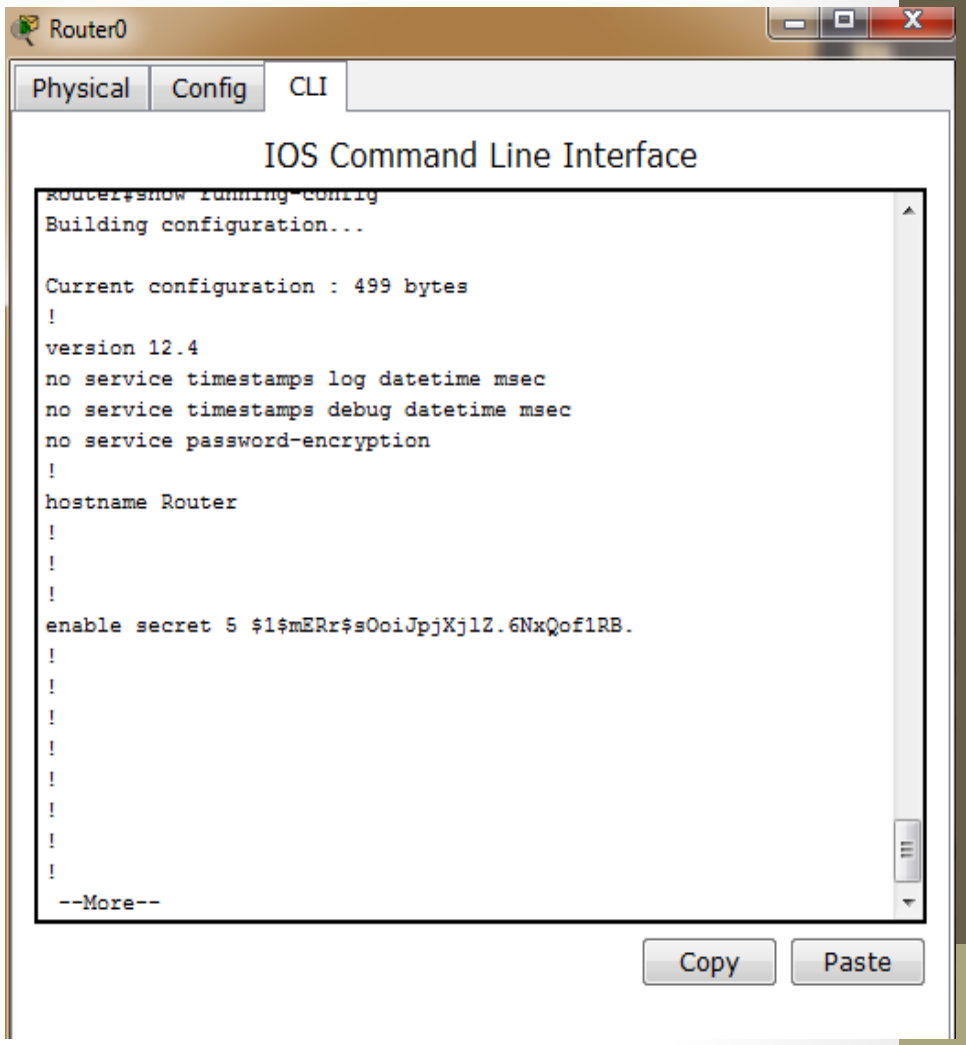
Setting an Encrypted Password

- To configure an encrypted password, type these commands, pressing the Enter key after each command:
  config t
  enable secret meow
  end

- To see the encrypted password, type this command, and then press the Enter key:

show running-config

The password is now hashed, as shown to the right on this page. Highlight the password hash as shown, right-click the highlighted area, and click Copy.



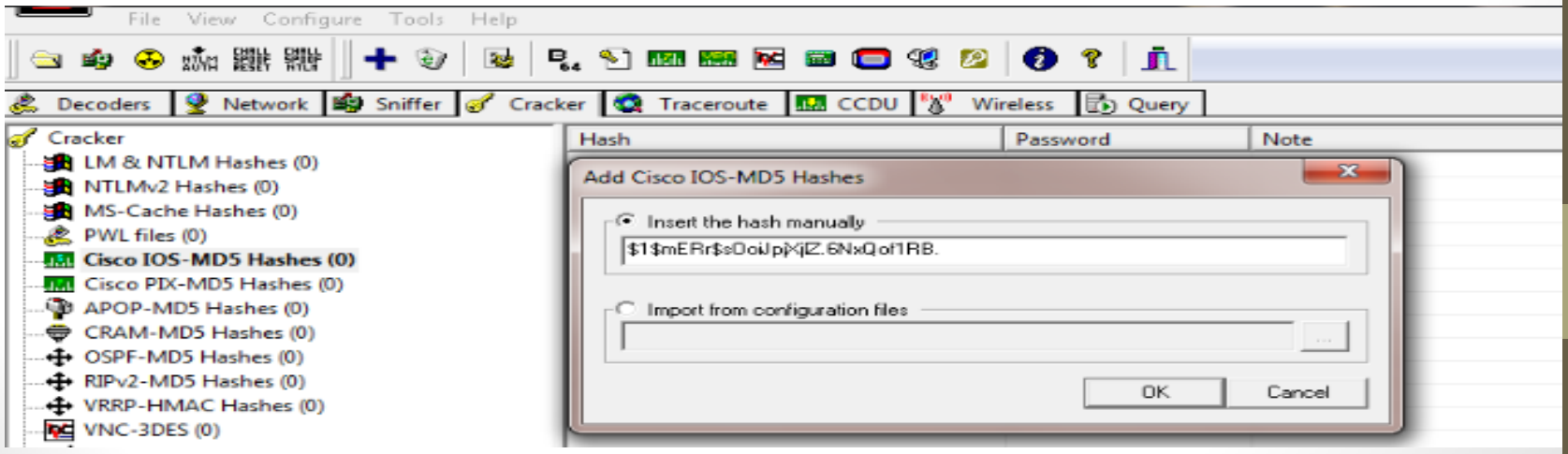
- Installing Cain If you don't already have Cain installed, download it from oxid.it/cain.html and install it:Right-click the Cain shortcut on your desktop and click "Run as Administrator“
- In the Cain window, click the Cracker tab. In the left pane, click the "Cisco IOS MD5 Hashes" item to highlight it.

From the Cain toolbar at the top of the window, click the + icon. An "Add Cisco IOS MD5 Hashes" box opens. Paste the hash into the upper box and click OK. The hash should appear in the central pane, as shown to the right on this page.

- In the central pane of the Cain window, right-click the hash and click "Brute-Force Attack".

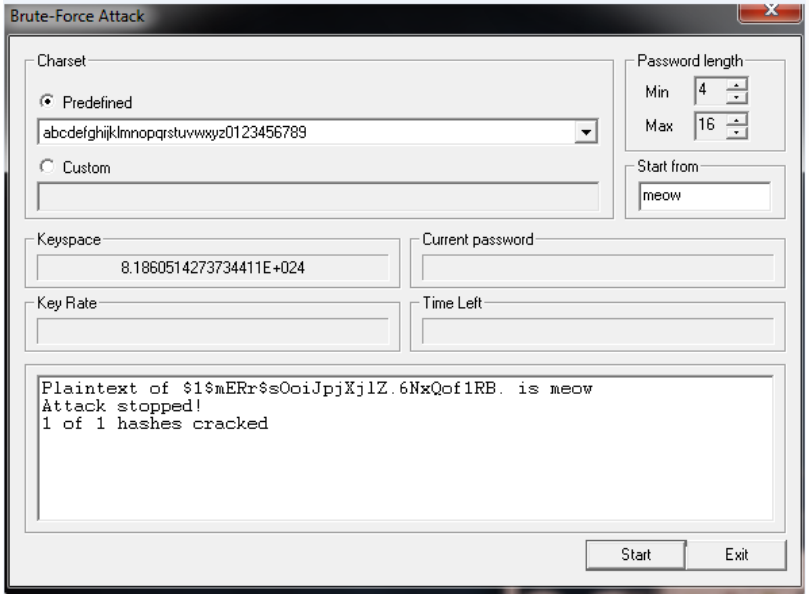
In the "Brute-Force Attack" box, click the Start button.

The password should be found in a few seconds, as shown on the next page of these instructions

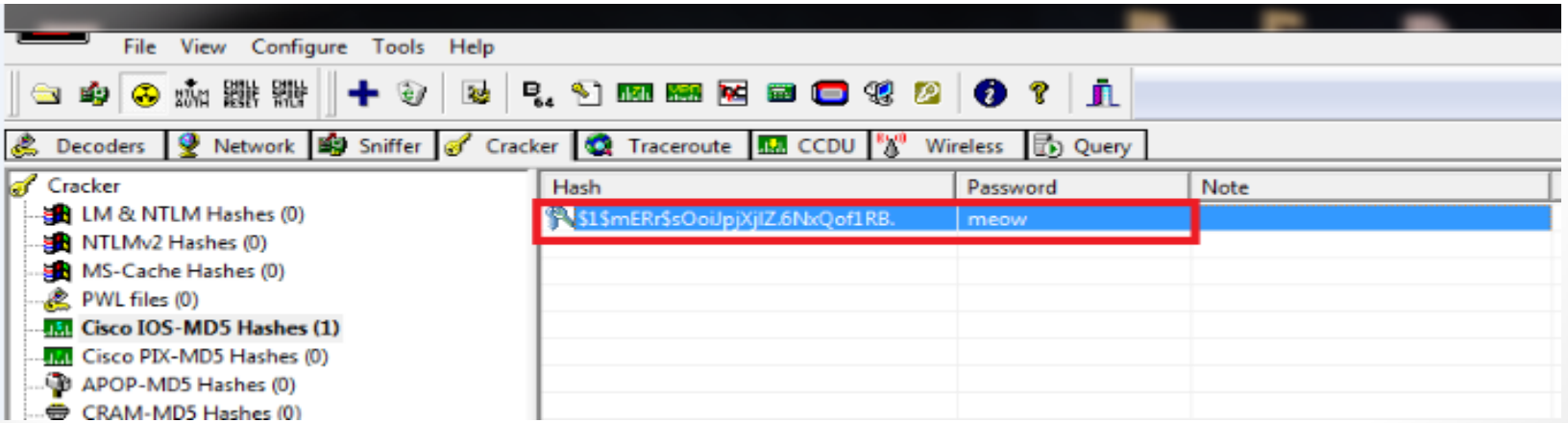


BRUTE-FORCE THE HASH AND GETTING PASSWORD MEOW

- In the central pane of the Cain window, right-click the hash and click "Brute-Force Attack". In the "Brute-Force Attack" box, click the Start button.



- Password successfully cracked shown below



@dodo


THANK
YOU