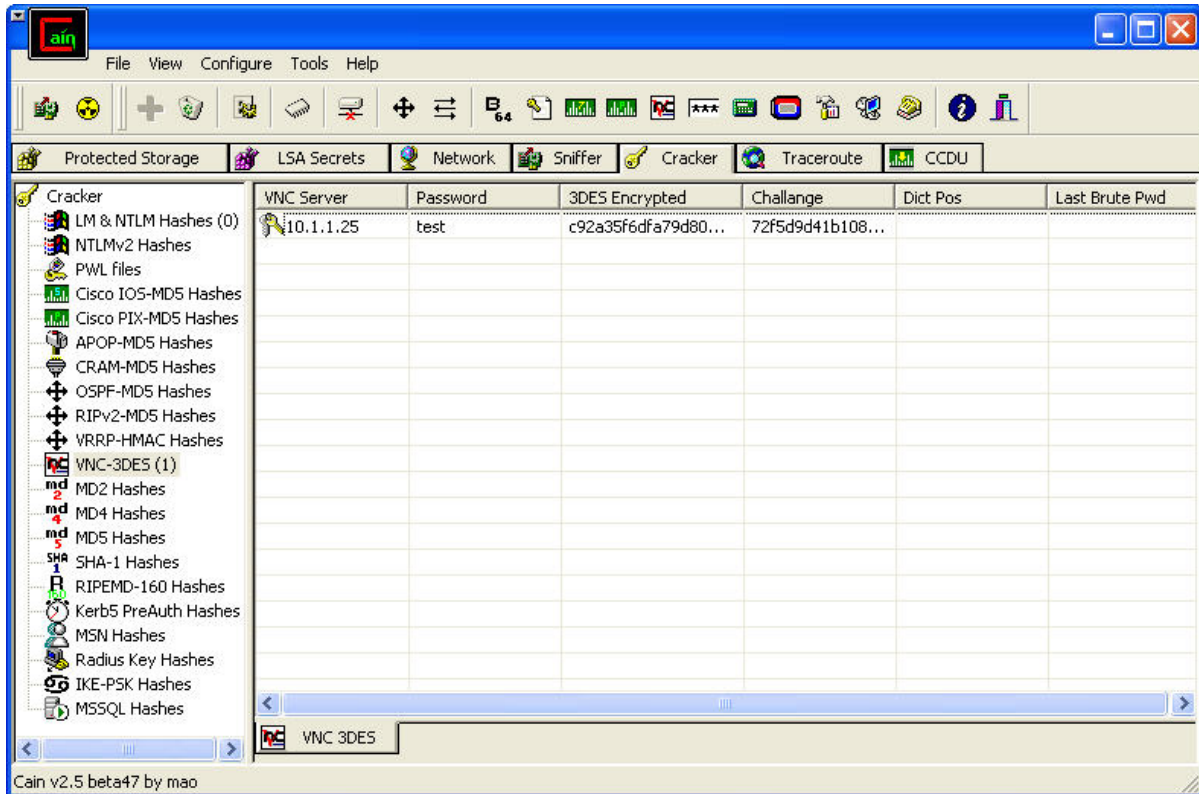


Using Cain



Laboratory Overview

Objective

At the end of this lab students will be able to use Cain's built in network sniffer to sniff out and crack VNC passwords.

Information for Laboratory

- A. Students will utilize VNC Remote desktop access software
- B. Students will utilize Cain Password recovery utility

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

Students will need to have VNC server service installed and running, the VNC viewer is available, and Cain installed and working.

Estimated Completion Time

60 Minutes

Network Sniffing for passwords

Ethernet networks transmit data to all stations connected to the same collision domain. Therefore, network sniffers located on the same domain as a server, can sniff important data that does not even belong to them.

Cain Password Recovery Utility



Cain and Abel version 2.5 is a utility used to recover lost



PRE-LAB SETUP

Step 1: Configure Cain

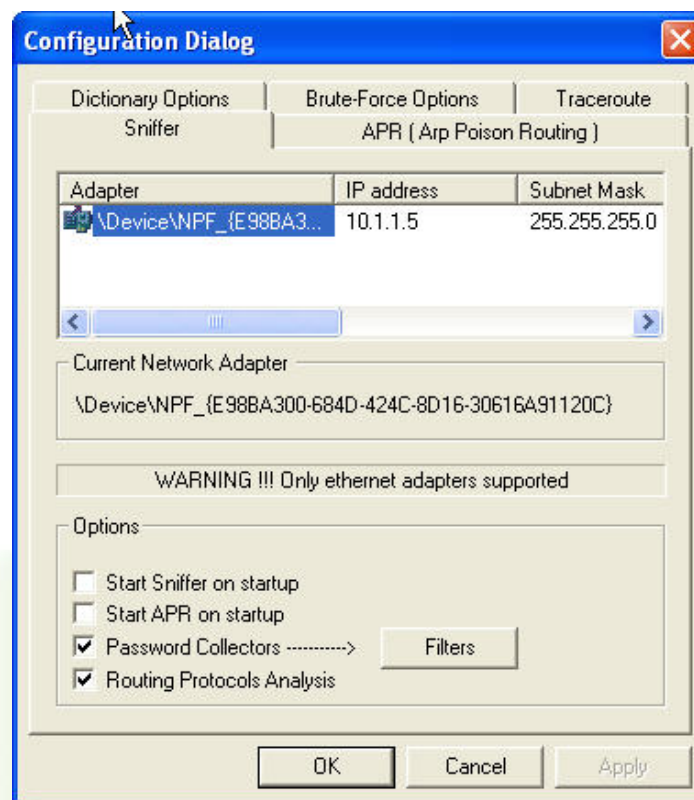
The screenshot shows the main window of Cain v2.5 beta47. The 'Cracker' tab is active, displaying a list of hash types on the left and a table of cracked hashes on the right. The table has five columns: 'User Name', 'LanMan Password', '< 8', 'NT Password', and 'LanMan Hash'. The 'LM & NTLM Hashes (0)' category is selected in the sidebar, and its corresponding entry is highlighted in the table. The status bar at the bottom indicates the version 'Cain v2.5 beta47 by mao'.

User Name	LanMan Password	< 8	NT Password	LanMan Hash

Cain v2.5 beta47 by mao



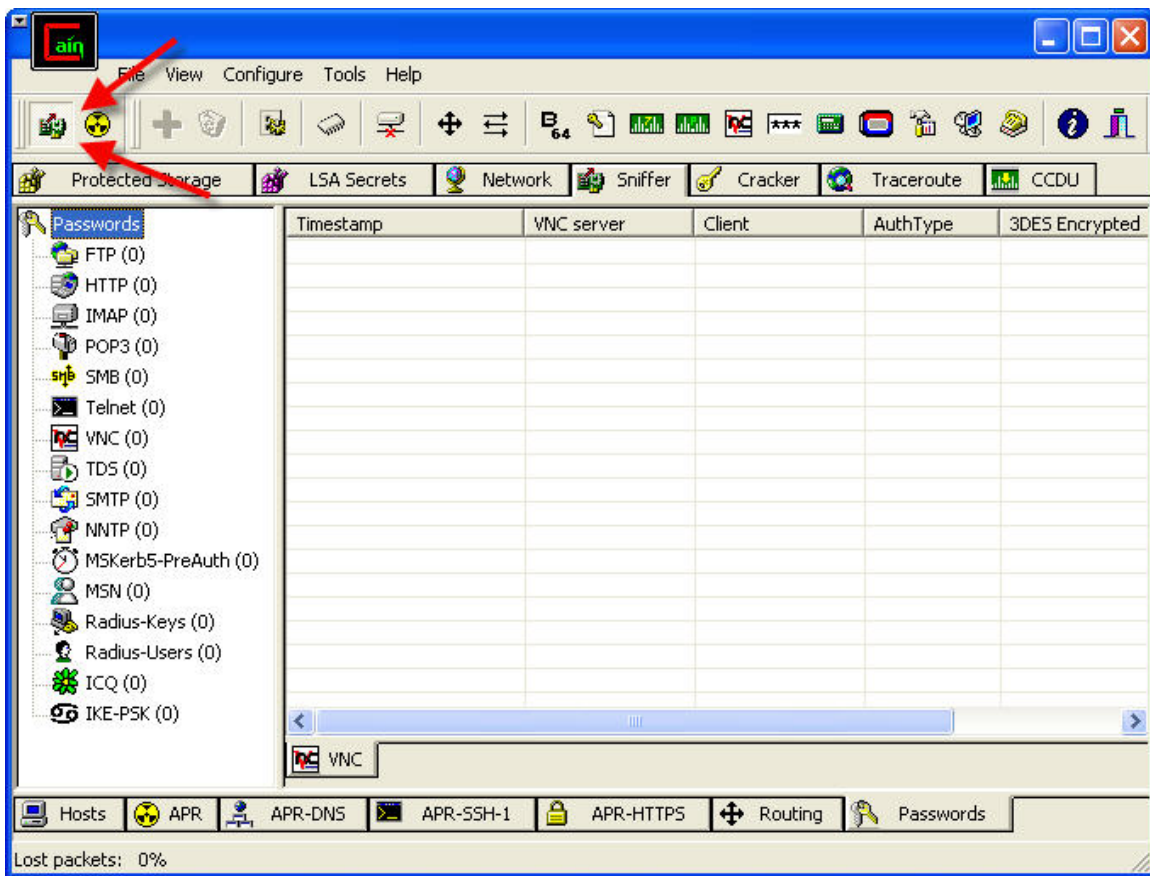
Click Configure on the top toolbar to launch the configuration screen.



Verify that the appropriate network card is selected on the Sniffer tab of the Configuration box. It should be the card with the correct corresponding IP address to the network you want to sniff on. Click ok when set.

Step 2: Enable Cain Sniffer

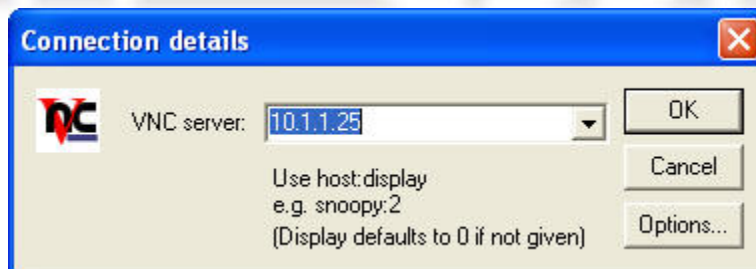
Click on the Sniffer tab on the top toolbar, and Passwords on the bottom toolbar, as below.



Verify that the Sniffer button is depressed

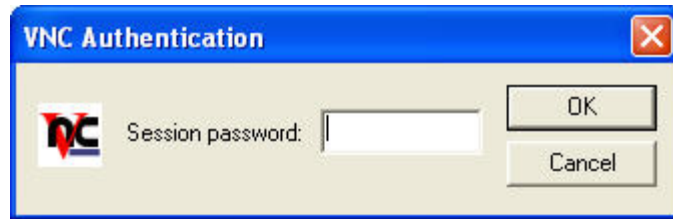
Step 3: Remote connect via VNC

From your workstation, launch VNC viewer as below.

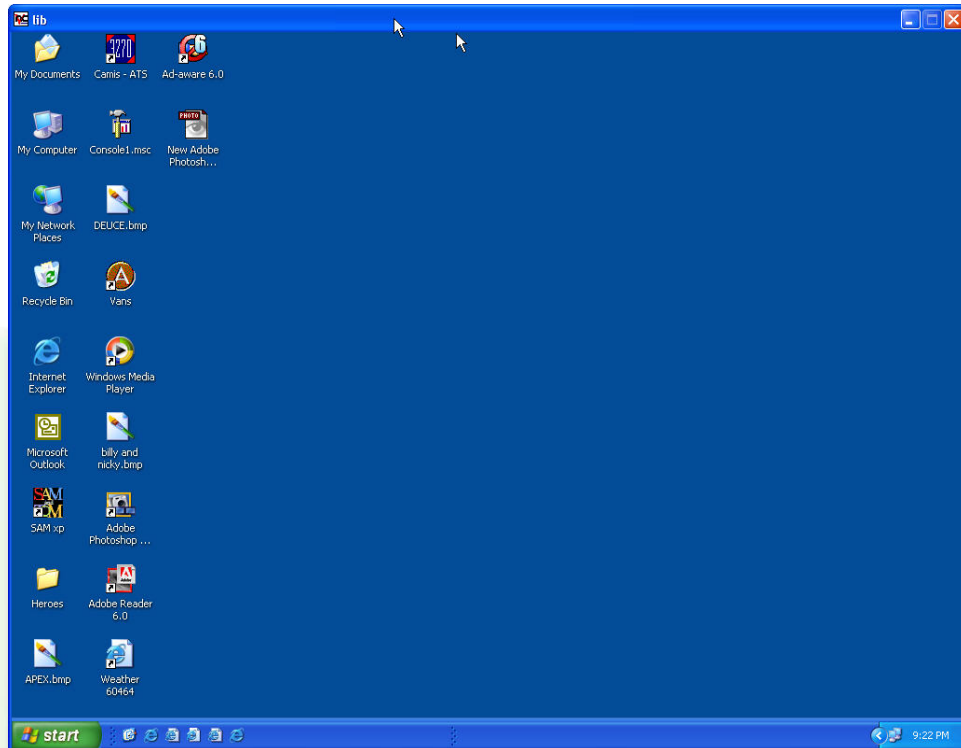


Enter the IP address of your partner or a second computer running the VNC server service, and click OK to connect to the remote computer.





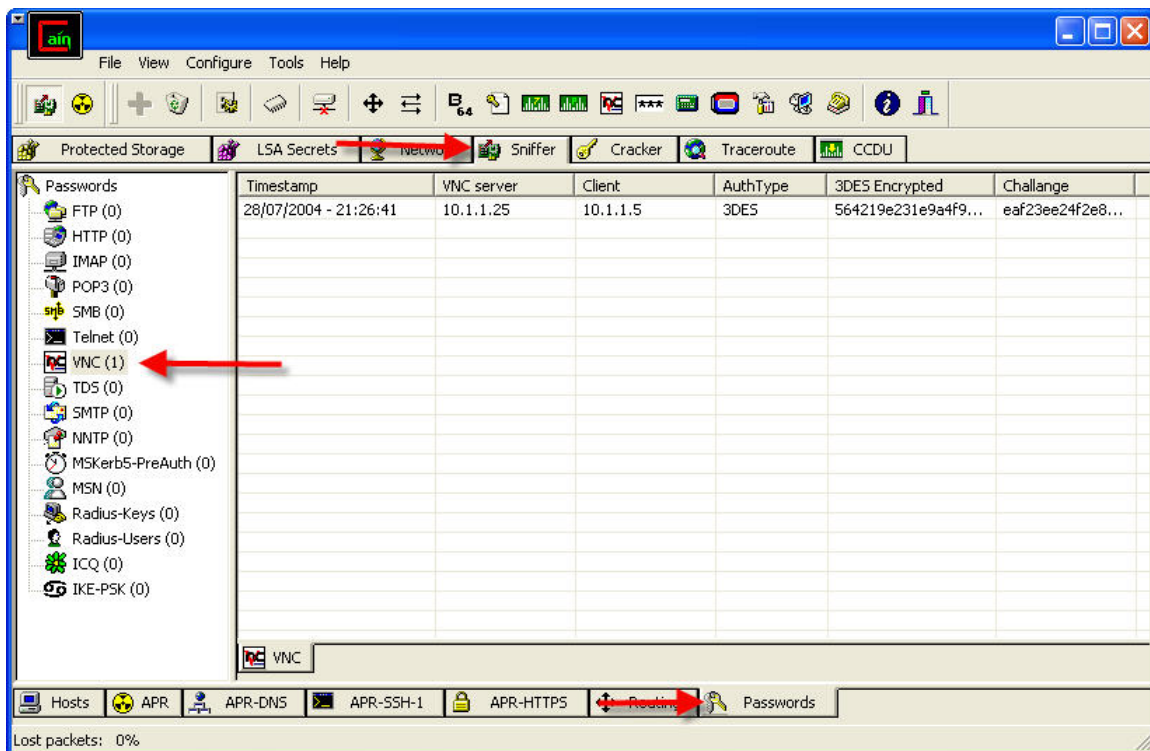
Enter the password in the dialog box.



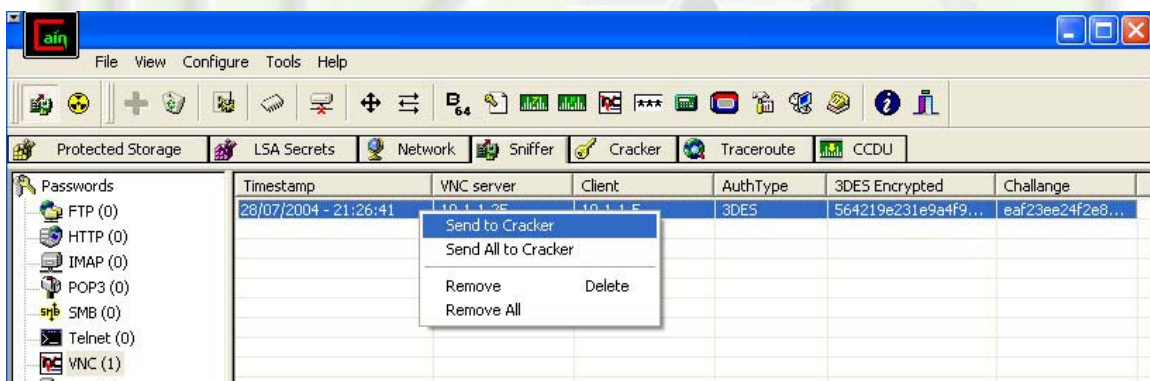
Once connected to the remote host, close the session and go back to Cain.

Step 4: Cracking the sniffed VNC password

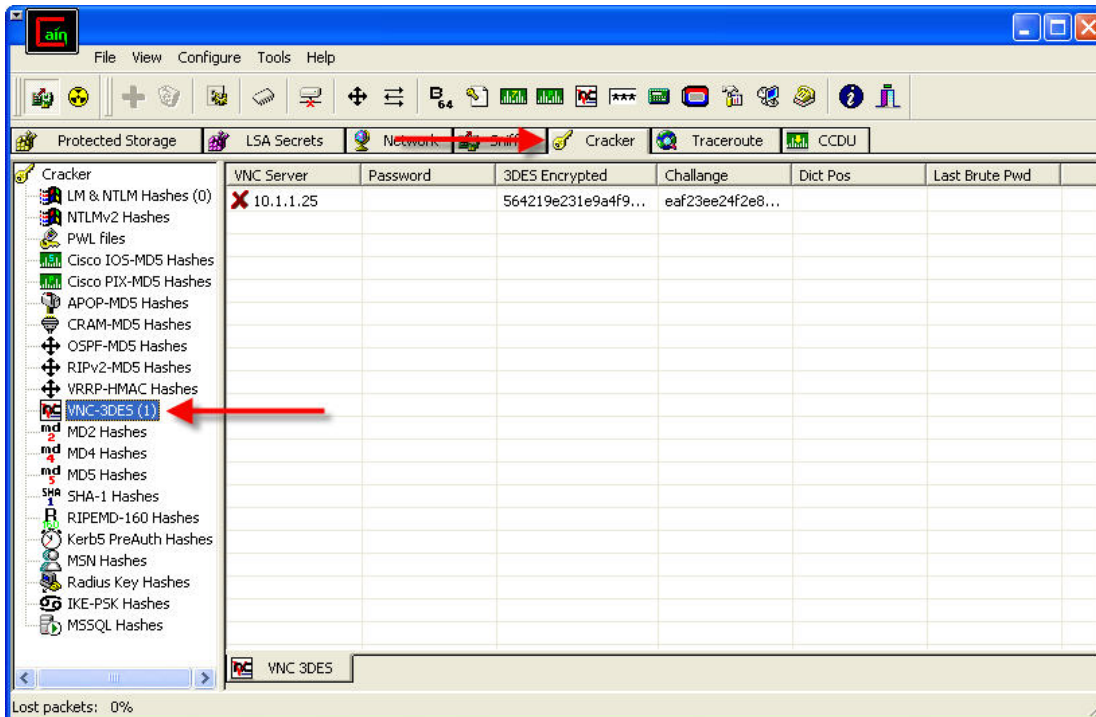
In Cain, navigate to the Sniffer, Passwords, VNC tab.



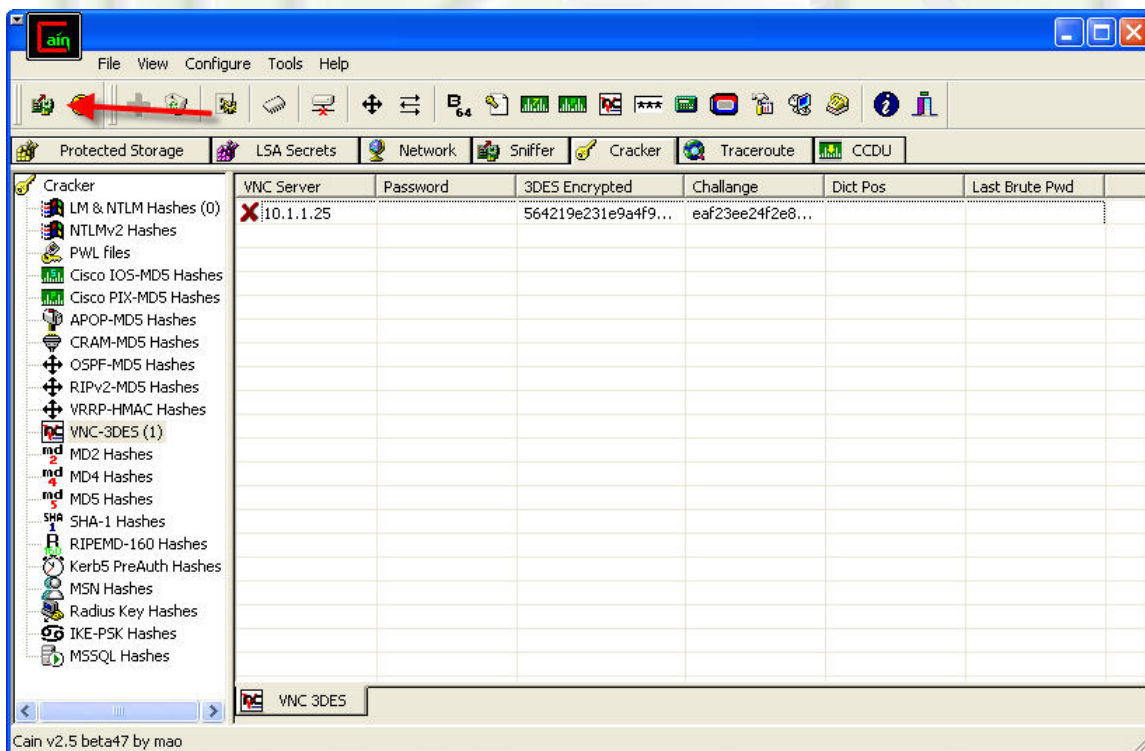
You should now have an entry in the window. Right click on the entry, and click Send To Cracker, as below.



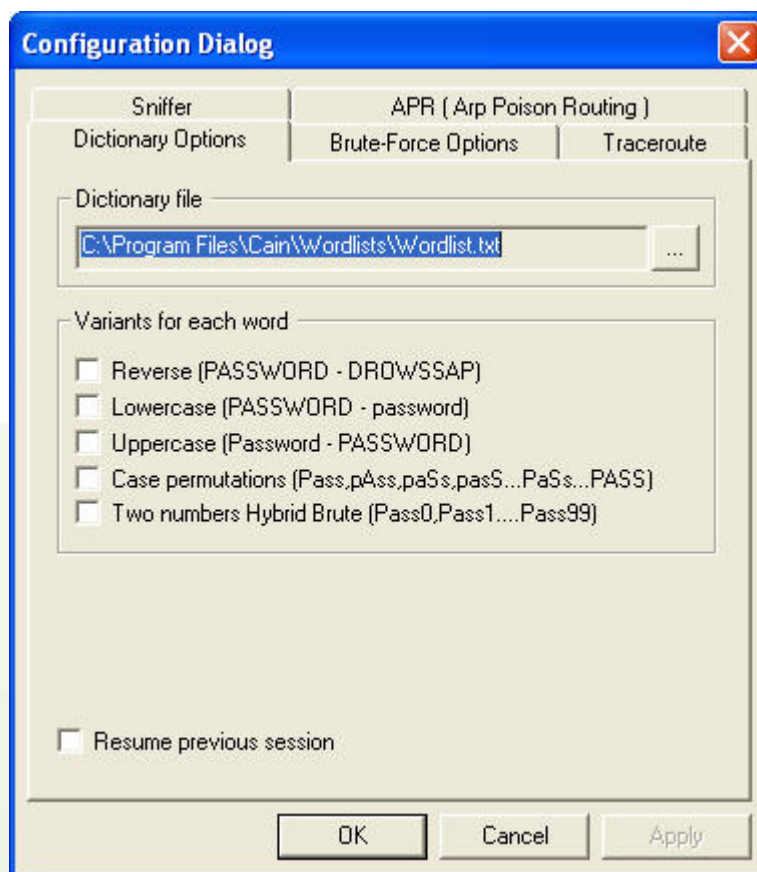
Click on the Cracker tab on the top toolbar, and VNC on the left side of the cracker screen as below.



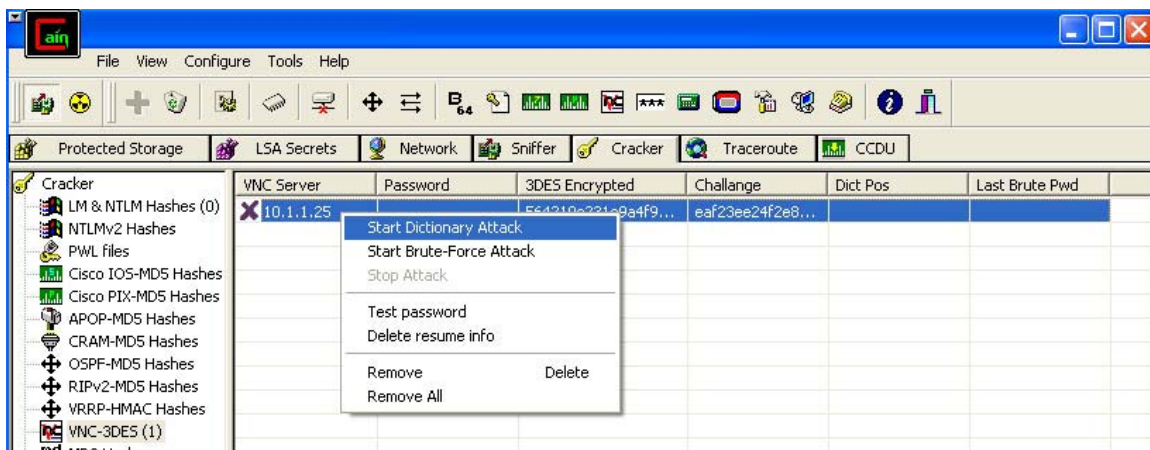
Verify that there is an entry in the cracker, and then Stop the Sniffer, as below. Click the Start/Stop Sniffer button.



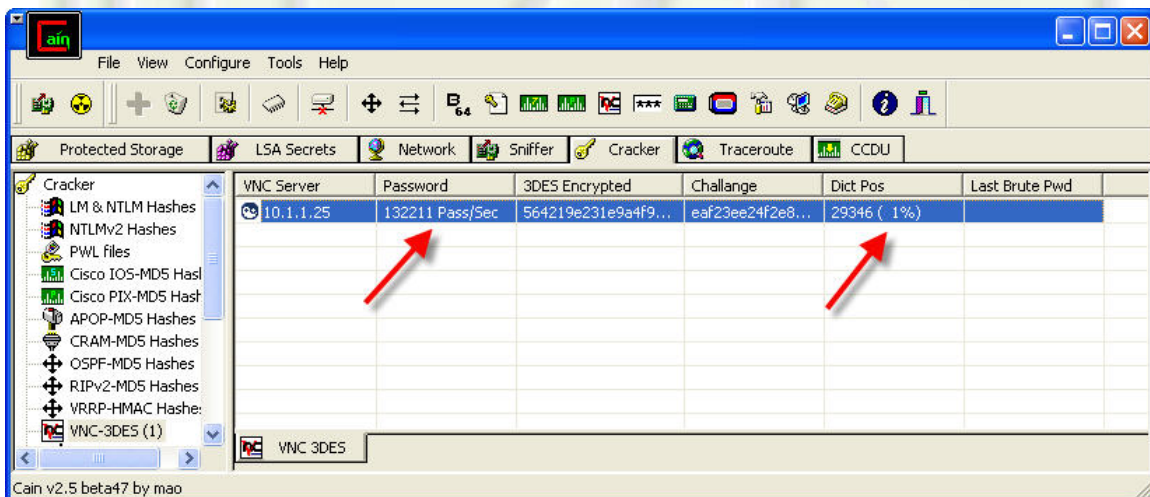
Depending on your Dictionary Attack options from The Configure menu, as below, this dictionary based attack could take a few seconds, to several minutes. Since we know the password is 'test', we want to undo all the options, only using the password list to minimize the cracking time.

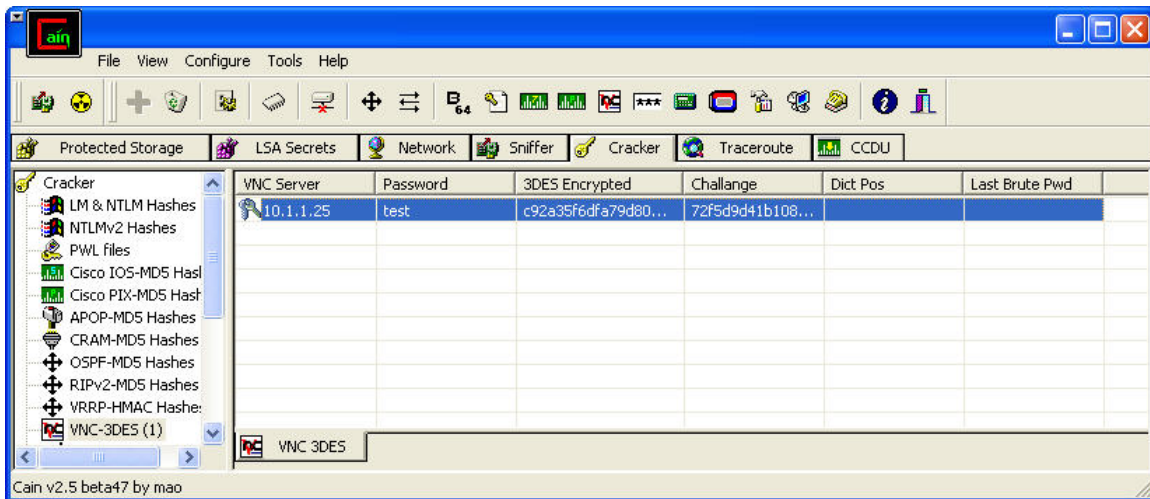


From the Cracker window, Right click on the entry in the cracker, and click Start Dictionary Attack, as below.



After starting the attack, let Cain run, depending on the password, this step could take several minutes. You can see the progress as below.





As above, when the cracker is finished, the password will be displayed in the password field. Verify that this is the correct password, and then close Cain.

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

Analysis

- 1) For which applications is network sniffing for passwords best suited?
- 2) After working with Cain, what about Cain do you feel you should study further? Why?
- 3) Why should you understand how hashes work to protect passwords?

If You Want To Learn More

Research the following terms:

- Password hashes
- Password hashing
- Cracking passwords
- Cracking password hashes

Appendix:

This lab was developed using Cain version 2.65, which can be obtained from:

<http://www.oxid.it>

Use the project link. An online manual is also available.

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04).

