Windows NT/2000 Password Cracking Laboratory – Module 8 Threats, Vulnerabilities and Attacks

Lab 1 – Bootdisk

Background: Password cracking is one of the most common attacks perpetrated against computer systems. With physical access and a special LINUX boot disk, it is possible to change passwords on a Windows NT/2000 system.

Requirements/assumptions:

- Windows NT 4.0/2000
- One 3½ inch floppy

In reviewing accounts on the network, you have encountered some that are questionable. While performing a more thorough audit, you have come to the conclusion that the employee who was recently dismissed created these. Upon further review, it is apparent that there may be some malicious software on his old workstation. To be sure, you must gain access to his Windows 2000 system, without his password. To accomplish this, you will be required to 'break in' to his computer. You have scanned the Internet, and found a tool that allows you to edit the password database on any Windows NT or 2000, or XP system. Here are the instructions:

Create the boot disk

1. Open an Internet browser and go to http://home.eunet.no/~pnordahl/ntpasswd/
2. Read the page, scroll to the bottom and click on the link to the Bootdisk: Instructions & image to download

**** Note: The instructors have made these files available locally and therefore in the interest of time, please access the below files from the \\192.168.30.250\sam network share. Simply copy the 2 required files from the instructors share into a c:\boot folder (you may have to create this folder first) and then follow the instructions starting at step 4.******

3. [This step is not required based on the note above, however it is left in place for student reference].

   Read this page and click the links to download the following files:
   a. When saving the files, **create a folder called c:\boot** and place both files in there
   b. bd011022.zip (it's 1.4 Mb)
   c. rawwrite2.zip (it's 10kb)
   d. Unzip these files and place the unzipped files into the same c:\boot directory

4. Open a DOS command line window (**Start | Run | cmd**)
5. Change to the c:\boot directory (c:\>cd boot)
6. Run the rawrite2 program
7. When prompted for the image source file name, enter 'bd011022.bin'
8. Enter a: as the target drive
9. Insert a formatted floppy into the a: drive and press enter
10. The boot disk is now being created
11. When the disk is completed, exit the DOS window
12. Remove the floppy and label it appropriately

Run against a system
(Note: It is very important to be careful when answering the questions as you run through this portion of the exercise, as incorrect selections may do serious damage to the OS)

1. Insert the disk into a floppy drive of a powered-down Windows NT or 2000 computer
2. Power On the system
3. The boot sequence starts with the boot disk (Linux)
4. When prompted, press enter
5. You will be confronted with the following questions. Default answers are depicted in []

    a. Probe for SCSI-drivers: [n]
    b. What partition contains your NT partition: [dev/hda1]
    c. Select what you want to do: [1] (which is set passwords)
    d. What is the full path to the registry directory: [winnt/system32/config]
    * * Note—You may have to change the path here, as it may default to an invalid [windows/… directory—type in the winnt/… directory as displayed above
    e. Which files do you want to edit: [sam system security]
    f. Do you really wish to disable SYSKEY? [n]
    g. Username to change: (Select one of the users from the list; Administrator is an acceptable choice)
    h. Enter the new password: (enter the password)
    i. Do you really wish to change it: [y]
    j. Username to change: [!] (This quits the password editor.)
    k. Write hive files? [y]
    l. About to write file(s) back! Do it? [y]
    m. Run ntfsfix to avoid problems with NTFS? [y]

6. You have now successfully changed the password
7. Remove the floppy and then Press Ctrl-Alt-Del to reboot

Test the new password

1. When Windows boots, enter the name of the account you changed
2. Enter the new password you entered with the utility

Lab 2 – Cain & Abel

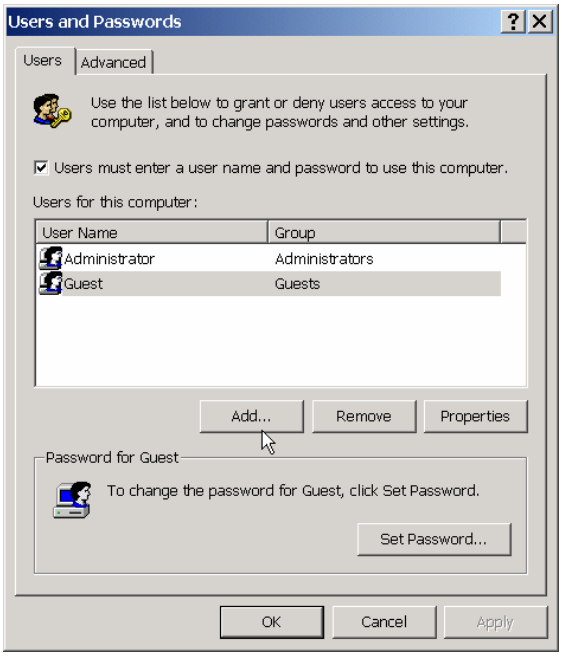
Background: Password cracking is one of the most common attacks perpetrated by intruders. Regular password auditing is a security best practice that all network administrators should conduct. There are many tools available for this purpose, however we'll use a free tool called Cain & Abel (henceforth Cain) produced by Massimiliano Montoro. Cain & Abel is a very powerful and multidimensional network auditing tool and can be hazardous if used inappropriately on production networks. As a result, we will be using it for local password cracking only.

Requirements/assumptions:

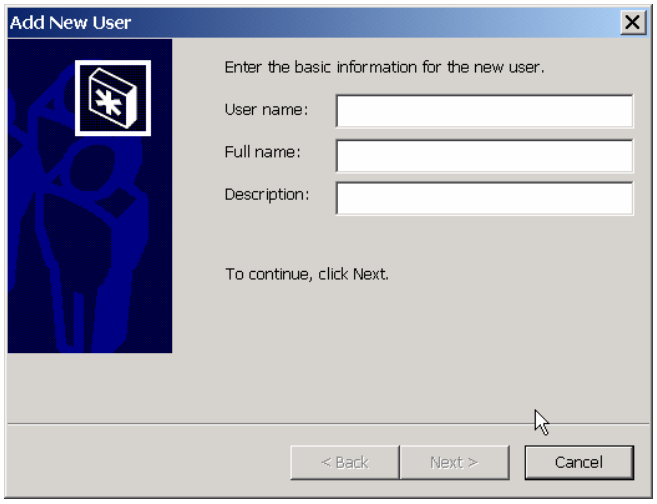
- Windows 2000/XP professional
- Cain & Abel (Cain) loaded on system (available at www.oxid.it)
- Administrator privileges on the system which Cain will be run

Create Accounts

1. Begin by creating a few accounts to test.
    a. To create user accounts, go to **Start | Settings | Control Panel**
    b. Double-click on **Users and Passwords**
    c. Click **Add** to add a new user



    d. When prompted, enter a user name (i.e. test1) and click **Next**.



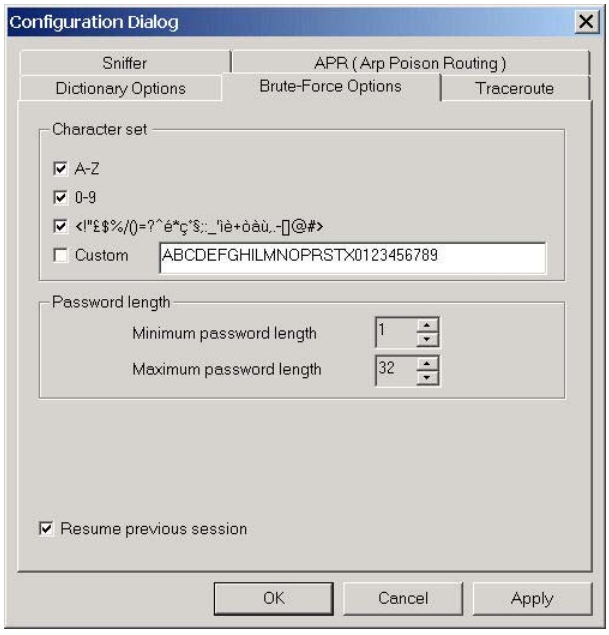
d. When prompted, enter the password for the new user. Use a short (3 letter) password that would appear in the dictionary, all in lowercase (i.e win). Click **Next**.

e. In the next window, select the type of user. Click **Finish**.

f. Repeat the process – incrementing the username by 1 each time (i.e test2, test3, test4, etc.) and using the following corresponding types of passwords:
   i. Longer dictionary word (i.e. confidential)
   ii. Short (4 letter) alphabetic password non-dictionary (i.e. hhfd)
   iii. Long alphabetic password non-dictionary (i.e. fhosjdowjemrog)
   iv. Short password with 1 numeral (i.e. h0t)
   v. Long password with numerals and/or special characters (i.e. N0guess1ng!)

Audit Passwords

1. Open Cain (visit www.oxid.it to download if needed)
2. Click on the Cracker tab, then click on **LM & NT Hashes** so that it is highlighted
3. Now click File| Add to list
4. Since we're concerned with passwords on this machine, select 'Dump NT Hashes from local machine' and click **Next**
5. Now **right click** on the first account you created (i.e. test1) and select **Start Dictionary Attack.** Now do the same exact thing for the second account you created (i.e. test2).
6. Next, **right click** on the third account you created and select **Start Brute-Force Attack**. Now do the exact same thing for the fourth and fifth accounts you created (i.e. test4 and test5)
7. For the last account you created, we are going to edit the attack options to include support for special characters. Click on the **Configure menu** and click **Brute-Force Options**. Under **Character set**, click the first three check boxes and then click OK. See screen shot below:



8. Now, right click on the last account you created and select **Start Brute-Force Attack**. It may take quite a while to crack complex passwords (sometimes days).