ScanNT Pro

Version 1.1

DO NOT USE THIS PROGRAM FOR ILLEGAL OR UNETHICAL PURPOSES!

Copyright

For more information contact *http://www.omna.com/Yes/MWC.*
Please send your questions and suggestions to *ScanNT@box.omna.com*

Requirements

The Windows NT 3.51 Intel version requires Windows NT 3.51 server or Workstation on Intel platform. Only Intel version is available at the moment.

Description

ScanNT (R) Pro version 1.1 is intended for use by system administrators in order to enhance the security of NT system. The program tests the sufficient complexity of the existing passwords.

After the program (*wscannt.exe*) is started, the main window appears.
Select: *accounts to scan*, *dictionary file* and *log file.*

How To:

SELECT ACCOUNTS TO SCAN

All Windows NT local user accounts appear in the left top box of the window in the control group "Accounts".

Select accounts to scan and press **[Add]** button in the "Accounts" group. The selected accounts will be transferred into the group "To Scan." To select all accounts and to to transfer them to the "To Scan" group, use **[>>>]** button. To remove the accounts from "To Scan" group, select them and press **[Remove]** button. Use **[<<<]** button to clear "To Scan" group.

SELECT A DICTIONARY FILE

Type the correct dictionary file name in the "Dictionary" text box within the "File" group. You can also browse your file system by pressing browse **[...]** "Dictionary" button.

SELECT A LOG FILE

Type the correct dictionary file name in the "Log File" text box within the "File" group. You can browse your existing file system by pressing **[...]** "Log File" button.

Check the "Append" radio button (default) if you want new results to be appended to the existing log file. Check "Overwrite" radio button to overwrite your existing Log File, if any.

SCAN

Start the password scan process by pressing the **[Scan]** button after you have selected the correct account names, dictionary file and log file.

The "ScanNT: Progress" dialog appears on the screen. You will see the current account name and the progress indicator in this dialog.

To interrupt the process, press the **[Cancel]** button and confirm interruption by pressing **[Yes]** in the appropriate dialog box.

Log file format

If the Scan process has been terminated normally, the Log File appears on the screen. The Format of the Log File appears as follows:

User1, message1
User2, message2
...
UserN, messageN, where:
UserK - the account name of the K-th user
messageK - the message for K-th user.

The messages are:
- OK (N attempts)
the password was not cracked after N attempts.
- Cracked! <password> (account temporarily disabled)
the password was cracked, but this account is temporarily disabled by the administrator.
- Cracked! <password> (unauthorized time of day for this account)
the password was cracked, but this time of day is unauthorized for this account.
- Cracked! <password> (the account is not authorized to logon from this station)
the password was cracked, but this account is not authorized to logon
from this station.
- Cracked! <password> (logon time restriction violation)
the password was cracked, but this logon time is unauthorized for this account.
- Cracked! <password> (password has expired)
the password was cracked, but the password has expired.
- account locked
the account is currently locked out and cannot be tested.
- account Cracked! <password>
the password was cracked. As an administrator you must prompt this user to change the password as soon as possible.

Error messages

<Username>, You must have SeTcbPrivilege privilege set.

Certain privileges must be set up for your account to successfully execute ScanNT program. The required privileges can be added to the account by using the "User Rights Policy" dialog box in the User Manager.

Run the User Manager and choose "User Rights" from the "Policies" menu to see the dialog box. Select the "Show Advanced User Rights" check box.
You must grant the following rights to execute ScanNT:

- "Act as part of the operating system"
- "Replace a process level token"
- "Increase quotas"

After you made this changes, you must logoff/logon for this account.

Tips

To achieve maximum number of logons per second, you must disable the security audit for user logon on your NT box. The simplest way to do this is to temporarily disable *EventLog Service* on your computer.

Due to the well-known bug in Windows NT (memory leak in the security subsystem), scanning large user databases and/or a large dictionary will drain virtual memory and slow down the system. To solve the problem, use the large paging file. To free virtual memory, reboot the system.

Copyrights

See readme.txt for distribution/license agreement information.

****