Copyright and Disclaimer

Written by: Andy Baron, Director of Technology, Midwestern Commerce, Inc.

This program uses intricate security features of Windows NT. Improper use of this program may result in damage to you system.

This program is supplied on as-is basis and Midwestern Commerce, Inc. shall not be held responsible for any misuse or damage it may cause to your or other systems.

For updates please visit
http://www.NTsecurity.com

Please send your questions and suggestions to
ScanNT@box.omna.com

Program 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 Window NT User Account passwords.

The program uses a plain text dictionary file as the file of assumed passwords to check if a password is sufficiently complex or easily breakable. ScanNT can check only local Windows NT accounts.

After the program is started, the main window appears.

Select **A*ccounts to Scan***, ***Dictionary File*** and ***Log File***.

To scan user account passwords against **Dictionary File**, click **Start.**

When scan is completed, results are written into **Log File,** which is automatically displayed.

System Requirements

ScanNT ® is a powerful password cracker for MS Windows NT ™ 3.51 and 4.0.

The Windows NT **Intel** version requires Windows NT 3.51 or 4.0 server or Workstation on Intel platform. Only Intel Version is available at the moment.

Alpha version or other custom versions of ScanNT can be built on request. Please contact *ScanNT@box.omna.com*

Required User Privileges

Certain privileges must be set 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 Window NT **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 these changes, you must **logoff** and **logon** for this account.

How to Choose Users to Scan

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

From the main dialog select an account(s) to scan and press **Add** button in the **Accounts** group. The selected account(s) will be transferred into the group **To Scan**. To select all accounts and to transfer them to the **To Scan** group, use **>>>** button.

To remove accounts from **To Scan** group, select them and press **Remove** button. Use **<<<** button to clear **To Scan** group.

How to Select a Dictionary File

Type the correct dictionary file name in the **Dictionary** text box within the **File** group.

You can browse your file system by pressing browse **…** **Dictionary** button to select a dictionary file.

How to Select a Log File

Type the correct log file name in the **Log File** text box within the **File** group. You can browse your existing file system by pressing **… Log File** button to select a log file.

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.

How to Run a Password Test

Start the password test by pressing the **Scan** button after you have selected the correct account name(s), 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

The following error message can appear in **Log File:**

<Username>, You must have SeTcbPrivilege privilege set.

Correction:

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

Open **User Manager** and choose **User Rights** from **Policies** menu to see the dialog box. Select **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 these changes, you must **logoff** and **logon** for this account.

Performance Tips

To achieve maximum number of logons per second, you must disable 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 large paging file. To free virtual memory, reboot the system.

Reporting Bugs

If you experience something you think might be a bug in ScanNT, please report it by sending a message to *ScanNT@box.omna.com*

Thank you.

Suggestion Box

Please send any suggestions or requests for new features to *ScanNT@box.omna.com*

Your input is always welcome and appreciated.

New in This Release

New features in ScanNT(TM) v 1.1:

Windows based utility is added.

"**-r**" switch is added to assign a priority for the process.

Restriction on the number of accounts to scan (3,000 in version 1.0) is removed.

New error messages are added.

Sample dictionary file (scannt.dic) is added to the distribution.

An option to change the file to be executed under service.exe is added.

Demo Version

The demo version of ScanNT has the following specific features:

ScanNT tries every suggested password with **00**, **01**, ..., **99** concatenated to the actual password that you provide in the dictionary file as well as the suggested password itself. Thus, the demo version works **101 times slower** than the Professional version.

The demo version of ScanNT tries all suggested passwords for all suggested accounts and will not stop the scan even if the account is cracked.

The demo version does not provide the cracked passwords (but it will tell you which account password was cracked).

A sample dictionary file contains **3,300 words** in comparison with **20,700 words** in the Professional version.