How to crack the *MS Windows NT 4.0 Server Evaluation*

Release Date: 14.Oct.1996
4xCD-ROM, 10/14/96, including Service pack 2, MS Outlook 97 and finally MS Exchange Server 5.0
Time Limitation: 120 days

Introduction:

Stenac (a Cracker) has offered tow Methods to crack the Windows NT 4.0 Server+IIS (English trial edition with 120 days time limitation). His first Method was based on replacing the "Schannel.dll" with his offered one. This solution had no success with the release, which I have (see above).

His second method was based on manipulating the file "NTOSKRNL.EXE" and registry. This method has seemed to be very nice. I was satisfied after reading his way to occupy the worker threads in order to replace some registry values. But in fact it is not possible to make changes to "NTOSKRNL.EXE". The system will not start, because there are some more checking methods (CRC32 ?) as only a simple checksum-test. So I was challenged to find another method.

You will find his methods under "nt4_trial.zip" and "nt4t-crc.zip" on cracker's Internet sites.

My Crack Algorithm:

NT 4.0 compresses the files contenting the "repair info" in repair directory, which will be written on repair disk. These files are named : sam._ , software._ , security._ , ntuser.da_ and system._ .
In compressed form you can't find something in these files, which could help you to find the location of registry values. But it is possible to use them as "expanded" files to repair Windows NT 4.0 Installation !

1) run rdisk.exe (Repair Disk Utility) and press "Update Repair Info", after updating the repair info let the program "Create Repair Disk".

2) make a copy of "system._" from your new repair disk on your hard drive, e.g. C:\ .

3) click on "START" button and select "RUN", type now: expand c:\system._ c:\system.txt and press "OK".

4) load the decompressed file "system.txt" in your hex-editor and search for the bytes:
   96 0B 60 54 00 60 33 6E
   and replace them with: 16 10 00 00 00 00 33 AC

5) search also for: 40 A5 1A E4 00 A3 02 00 99 2B BC 01
   and replace them with: F0 46 4C A1 00 00 00 00 1B F6 BB 01

6) rename the changed file "system.txt" to "system._" and overwrite the one on your new repair disk with this uncompressed and newly changed one. Note that you can't save the new "system._" on a 1.38 MB Floppy, if your repair info files are grown up by installing a lot of software on your computer.

7) shutdown your computer and start with SETUP DISK 1 (there are 3 installation floppy disks in the Windows NT 4.0 Operating System Software Package) in order to "repair" the Windows NT 4.0 Installation by using the repair disk. After reading disk 1 put disk 2. A dialog screen appears, press "R" (To repair a damaged Windows NT version 4.0 installation, press R). After pressing "R", at the next dialog screen select cross only "INSPECT REGISTRY FILES" and continue as usual. A new dialog screen appears :

   "Setup needs to know if you have the Emergency Repair disk ..."

   press ENTER and put your repair disk in floppy drive. On the last dialog screen (Setup will restor each registry file...) cross only SYSTM and continue.

Now the correct values are in the registry and the 120 days limitation is not more active. Many thanks to Stenac for his registry values. His methods could not help me, but without his values I could not realize this crack.

Have fun using NT-Server, Masdak