HOW TO GET ANY WINDOWS PASSWORD

//////////*1000+ HACKING TRICKS & TUTORIALS - ebook By Mukesh Bhardwaj Blogger - Paid Version - only @ TekGyd | itechhacks | Mukeshtricks4u*///////

---

ok..... here are the full details.....

this works whether its windows 2000 or windows xp or windows xp SP1 or SP2 or windows server 2003....

this works even if syskey encryption is employed...

if it is FAT filesystem...

just copy the sam file like stated in the first post to an empty floppy disk and take it home. I'll tell u what to do with it later... DON'T DELETE THE ORIGINAL SAM FILE. just remove its attributes. the sam file is a file called SAM with no extension. YOU MUST ALSO GET.... a file called SYSTEM which is in the same folder as SAM. both files have no extensions...

if it is NTFS....

u have to download a program called NTFSPro.... it allows u to read from ntfs drives... the demo version allows read only. the full version is read-write.... you use the program to create an unbootable disk (so u will still need another bootable disk and an empty disk) that has the required files to access NTFS.

use the boot disk to get into dos, then use the disks created with ntfspro to be able to access the filesystem, then copy the SAM and SYSTEM files to another empty disk to take home....

AT HOME: u have to get a program called SAMInside. it doesn't matter if it is demo version. SAMInside will open the SAM file and extract all the user account information and their passwords, including administrator. SAMInside will ask for the SYSTEM file too if the computer you took the SAM file from has syskey enabled. syskey encrypts the SAM file. SAMInside uses SYSTEM file to decrypt the SAM file. After SAMInside finishes, u still see user accounts and hashes beside them. the hashes are the encoded passwords. Use SAMInside to export the accounts and their hashes as a pwdump file into another program, called LophtCrack. it is currently in version 5, it is named LC5. the previous version, LC4 is just as good. u need the full or cracked version of the program. LC5 uses a brute force method by trying all possible combinations of letters numbers, and unprintable characters to find the correct password from the hashes in the pwdump file imported into it from SAMInside. This process of trying all passwords might take 5 minutes if the password is easy, up to a year if the password is long and hard (really really hard). LC5 howver, unlike LC4, is almost 100 times faster. both can be configured to try dictionary and common words before using all possible combinations of everything. Once the correct password is found, it will display the passwords in clear beside each account, including administrator.

I use this method so many times. I've compromised the whole school computer infrastructure. LC4 usually took between 1 second and 10 minutes to find the passwords because they were common words found in any english dictionary. I haven't used LC5 yet.

If there is anything unclear, anything I overlooked, plz tell me so that I can turn this into a very easy to follow tutorial to help anybody crack any windowz pass.

Programs needed: SAMInside (doesn't matter which version or if demo)
LC4 or LC5 (lophtcrack)(must be full version)
NTFSPro (doesn't matter if demo)
any bootdisk maker

Cracked or full version software can be found on any warez site. If u don''t know what that is or where to get the programs, post a message and I'll tell u or give them to u.

P.S: I might not keep track of this forum, because I'm going to create a new topic and post tutorial there. if u want to post, plz post there.