

# Information Assurance Meeting

## September 13, 2005

### Agenda

- Remarks – Dr Ezekiel
  - Presentation: Windows Passwords – How they are stored, Resetting, & Cracking
  - Finish discussion of agenda
  - Other Business
- 

### Windows Passwords

Windows password is stored, by default, in a non-secure way. It is stored in the SAM file, which is located at: C:\WINDOWS\system32\Config\ Inside the SAM file, passwords are encrypted in LM (LAN Management) hashes.

#### Securing Windows Passwords

To secure your Windows passwords you'll need to make a registry edit.

1. Click the "Start" Button
2. Select "Run" and type "regedit" and click "OK"
3. Go to the following location:  
My Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentcontrolSet\Control\Lsa
4. Find the "nohash" key and open it
5. Change the "Value data" from 0 to 1
6. Close the key and exit the registry editor

#### Cracking Windows Passwords

To do this, you will need a live linux distro that will run off of a CD (i.e. Knoppix) and a thumb drive.

1. Boot the computer from the live linux distro
2. Mount the thumb drive
3. Copy the SAM file from mnt/sda1/WINDOWS/system32/config to mnt/uba1/ (your thumb drive)
4. Go to your computer that has Sam Inside and L0ftcrack installed
5. Extract the password hashes from the Sam file with Sam Inside
6. Open the password hashes with L0ftcrack and let it run
7. Come back after a few hours or days and the passwords should be cracked

## **Resetting Windows Passwords**

You will need to download and create the Offline NT Password Editor boot disk, see links below.

1. Boot the computer using the Offline NT Password Editor boot disk
2. Select 1 – “Edit user data and passwords”
3. Select “Administrator” – or the user account you wish to change
4. Enter “\*” to reset the password to blank
5. Type “y” and hit enter to make the changes
6. Type “q” to quit
7. Type “y” and hit enter again to commit the changes
8. Remove the disk and restart the computer
9. Login using the changed user account and leave the password blank