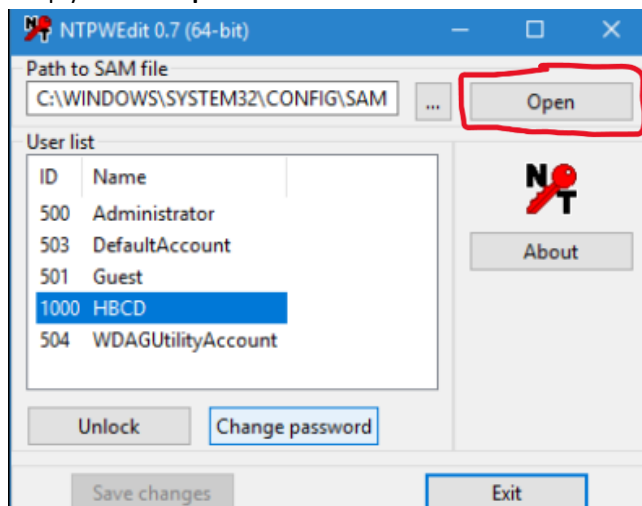


SYSTEM HACKING

- ➔ Exploiting Services and outdated software
- ➔ Password Cracking
 - Windows
 - Linux

WINDOWS CRACKING

- ➔ With bootable windows OS
 - First of all make a bootable pendrive with windows ISO
 - Restart the system go to the boot menu and select your bootable pendrive
 - Once the installation window opens press **shift + F10(to open cmd)**
 - Switch to c drive by typing **C:**
 - Cd windows/system32
 - Ren osk.exe osk1.exe
 - Copy cmd.exe osk.exe
 - Close the cmd
 - Close the installation windows
- **Open On screen keyboard from accessibility feature**
 - **Net user** (to check the available users)
 - Net user username * (It will ask to enter a new password)
 - Close the cmd
 - Login with new password
- ➔ Hiren Boot
 - Make a bootable pendrive with hirenboot ISO (<https://www.hirensbootcd.org/download/>)
 - Restart the system and go to the boot menu
 - Boot with your bootable pendrive
 - Once the Hirenboot os is started
 - Simply search **nt password**



- Click open button

- **Select user and click the change password button**
- **Then restart (remove the bootable pendrive)**

LINUX PASSWORD CRACKING

- ➔ Restart the system
 - ➔ Press **e** while it load grub boot loader
 - ➔ Go to the linux line
 - ➔ Replace ro quite splash with rw init=/bin/bash
 - ➔ Ctrl + x
-
- ➔ Once the root terminal opens
 - ➔ Type: mount -o rw,remount /
 - ➔ Ls /home (to find out existing users in OS)
 - ➔ Passwd username (it will ask for the password)