Help!
I'm locked out of my computer!

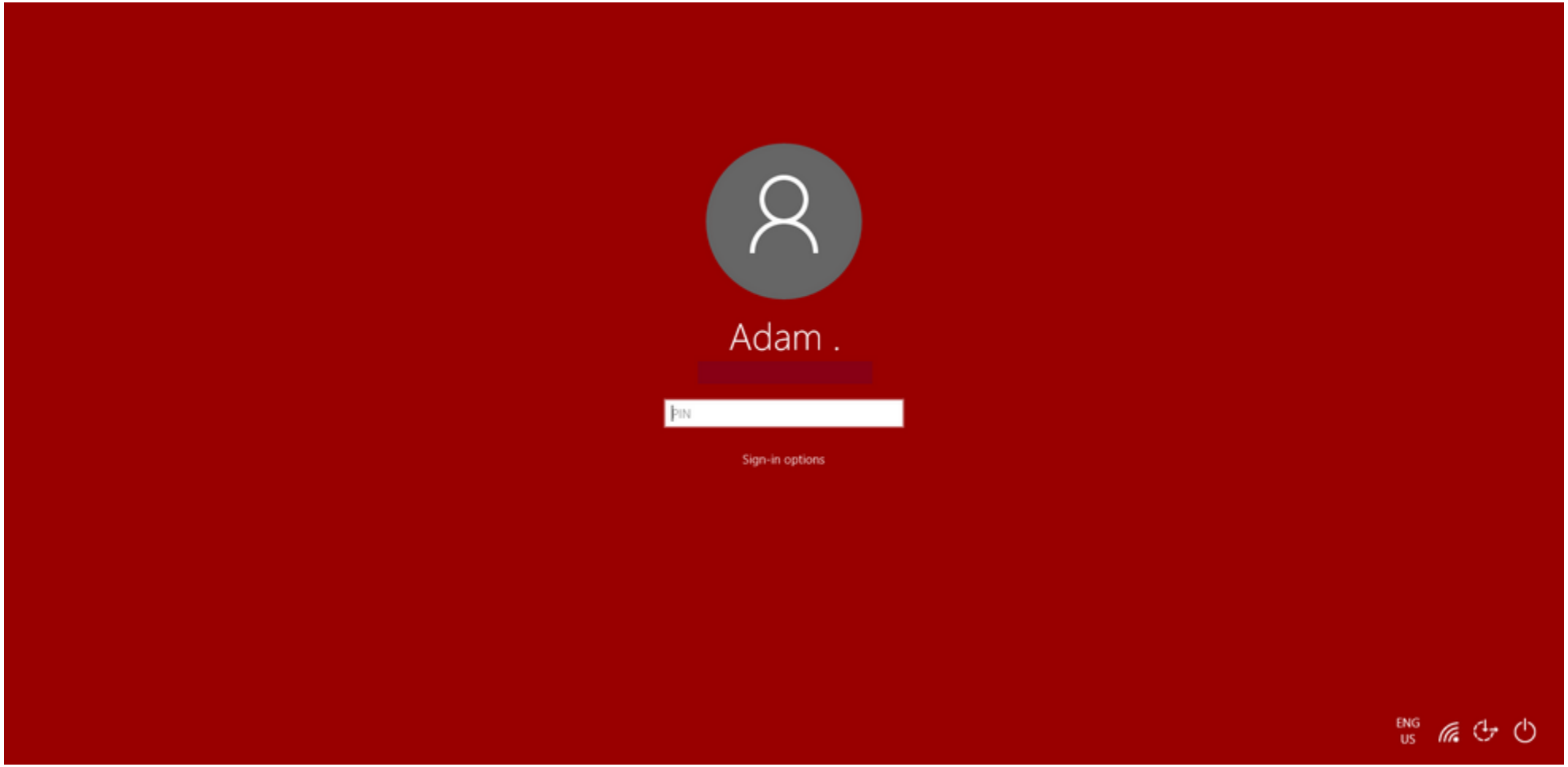
What do we mean by “locked out”? Forgot password

- Email account
  - You're on your own: contact Verizon or Comcast or use lost email procedure on email Web site.
- Local account
  - Cracker CD: e.g., Offline NT Password & Registry Editor
- Microsoft account
  - This is the tough one!

Getting Access to Microsoft Account

- Strategy
  - Create a new administrative account (name: rescue)
  - Copy data from locked Microsoft account into the “rescue” account
  - Delete the locked account
  - Rename the rescue account to any name desired

You are stuck at the login screen



Notice the small “Ease of Access” icon

Geeky Stuff - Tactics

We need access to the command prompt with administrative (elevated) privileges

- We will “reprogram” (re-purpose) the Ease of Access icon so that it produces a command prompt with administrative privileges.
- Then, with two lines of code, we will create a new administrative user (we'll call him “rescue”).
- Copy the data from the locked account into “rescue.”

Reprogramming Ease of Access Icon

- Boot with Linux Live CD or flash drive – any type of Linux is okay.
- Open the Linux file manager.
- Navigate to “Local Disk” or whatever you have called it in Windows.
- Navigate to /windows/system32 folder.

Reprogramming Ease of Access Icon

- Once in /windows/system32, locate the following file: utilman.exe (that is the program for Ease of Access.
- Rename utilman.exe → utilman.bak
  - (Remember to put things back to the way they were when we have finished).
- Locate cmd.exe
  - This is the elevated command prompt.
  - Copy cmd.exe to utilman.exe

(This reprograms Ease of Access to the command window.)

Now, Let's Go

- Reboot into Windows, where we are again stuck at the login screen.
- Click the Ease of Access icon. It now opens an elevated command prompt (\windows\system32).
- Type the following two commands:

```
net user rescue /add

net localgroup administrators rescue /add
```

It's Showtime

- Reboot again – to the login screen.
- Click the icon for the “rescue” account in the lower left hand corner.
- You are in!
  - Navigate to the Microsoft account.
  - Copy each folder to a corresponding folder in the rescue account (e.g., Documents → Documents; Pictures → Pictures)

Forgetmenots

- Now that you are “saved,” reboot into Linux and change utilman back to its original purpose (i.e., delete utilman.exe; rename utilman.bak to utiliman.exe)
- And finally:

Make a record of the bloomin' password!

Commercial Recovery Products

- Windows Password Recovery Tool Ultimate: $44.95
- SmartKey: $44.95
- Windows Password Genius Advanced: $49.95
- PCUnlocker: $19.95