Overview

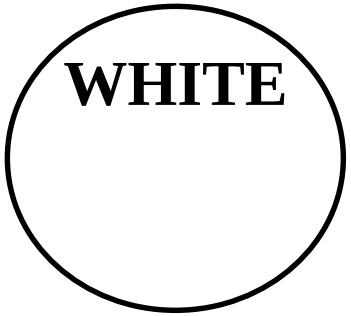
- Before

PoliticsPolitics

In-house tools

- Used WinBatch (www.windowware.com) to create 20 custom tools

Fig 2 - Re-SID’ing the w2k standalone



Giving notice

Crack

Crack

- In-house migration tools and ADMT would not migrate account passwords
- Process
- **Results**

Backup 4.0

Backup w2k

- Brought standalone w2k server into AD
  - Installed DDNS
    - Zone authority for all xxx.w2k.vt.edu

Edit web page tool

Monitor logs

- Turned on logging for the following logs:
  - Account logon events [fail]
  - Account management [fail,success]
  - Directory service access [fail]
  - Logon events [fail]
  - Policy change [fail,success]
  - Privilege use [fail]
- Filled up security event log VERY quickly.

Building new OUs

- Process for IRM to add new users to AD
  - OUs not already existing are created on the fly
  - Based on DNS on user's desktop machine
- Automated OU creation and user moving

Security pitfalls

- Anonymous users can not enumerate accounts
  - Unlike NT 4.0
  - Decided this when installing AD
  - Added the Everyone account to “Pre-Windows 2000 Compatible Access” group
  - Guest is still disabled
- Authenticated users can add workstations to the domain (w2k default) – whoops!
- Enterprise admins must authorize use of w2k DHCP in AD (can be delegated)