Windows 2003 Checklist

IF PATCHES ARE AVAILABLE INSTALL IMMEDIATELY

* DISABLE LMHash:
  + Click the START button
  + Click “Run”
  + Type “regedit” and click OK (this will open the registry editor, be careful in here only change what is mentioned)
  + Click the plus arrow to expand the HKEY\_LOCAL\_MACHINE tree (from now on said as expand [tree name])
  + Expand the SYSTEM tree
  + Expand the CurrentControlSet tree
  + Expand the Control tree
  + Click the Lsa directory
  + Double click nolmhash
  + Change the value “0” to “1”
* SET PASSWORD POLICY
  + Click START
  + Administrative Tools
  + Domain Security Policy
  + Click ‘Account Policies’
  + Click ‘Password Policy’
  + Ensure ‘Enforce Password History’ is set to 0
  + Ensure ‘Reversible Encryption’ is DISABLED
  + KEEP WINDOW UP
* CHANGE ADMINISTRATOR PASSWORD --- HANDLE USERS
  + Click start
  + Go to programs
  + Go to administrative tools
  + Click Computer management
  + Click Local Users and Groups
  + Double Click Users
  + Find your administrator account (There should only be 1)
    - IF there are OTHER administrator accounts right click THEM
    - Click properties
    - Click the “Member Of” tab
    - Click the “Administrators” group
    - Click the “Remove” button
    - Click the “Apply” button
    - Click back to the “General” tab
    - Click the “Account is disabled” checkbox
    - Repeat for any other administrator accounts
  + Right click your administrator account
  + Click “Set Password”
  + Change the password to your desired password
  + Go through all other non-admin user accounts and:  
     1) Right click the user

2) Click “Properties”

3) Click the “Account is disabled” checkbox

4) Click the “Apply” button

* FIREWALL
  + Click START
  + Control Panel
  + Right click and Open ‘Network Connections’
  + Right click a ‘Local Area Connection’ select ‘Properties’ (There might be multiple, repeat for all)
  + Go to ‘Advanced’ Tab
  + Enable Firewall then click ‘Settings’
  + Based on what is needed for the BOX, go through tabs and select what you need
* Disable Unnecessary Services (UNNECESSARY SERVICES TO DISABLE GUARANTEED: PRINT SPOOLER)

1. Click start
2. Go to “Programs”
3. Go to “Administrative Tools”
4. Go to “Services”
5. Right click the desired Service
6. Ensure the “Recovery” tab has all failures set to “Take No Action”
7. Click the “Apply” button
8. Return to the “General” Tab
9. If it its running (it likely will be) click the “Stop” button
10. Click the “Startup type” drop down box
11. Click “Disabled”
12. Go the “Apply” button
13. Click the “Log On” tab
14. Click the desired Profile (preferably all of them)
15. Click the “Disable” button
16. Uncheck the “Allow service to interact with desktop” checkbox if so desired
17. Click the “Apply” button

* SET ACCOUNT LOCKOUT POLICIES
  + Window should still be up for Domain Security Policy
  + Click ‘Account Policies’
  + Double Click ‘Account Lockout Policy’
  + Change ‘Lockout Duration’ to 1 minute
  + Change ‘Account Lockout Threshold’ to 5
* TURN ON AUDIT LOGS
  + Window should still be up for Domain Security Policy
  + Click ‘Local Policies’
  + Click ‘Audit Policies’
  + Enable for ‘Success’ and ‘Failure’ for all audits on the right
* Security Configuration and Analysis
* Sandboxie
  + <http://www.sandboxie.com/index.php?ClosedKeyPath>
  + <http://www.sandboxie.com/index.php?FrequentlyAskedQuestions>