Windows 2000 Checklist

IF ANY PATCHES BECOME AVAILABLE INSTALL THEM IMMEDIATELY

1. DISABLE LMHash:
   1. Click the start button
   2. Click “Run”
   3. Type “regedit” and click OK (this will open the registry editor, be careful in here only change what is mentioned)
   4. Click the plus arrow to expand the HKEY\_LOCAL\_MACHINE tree (from now on said as expand [tree name])
   5. Expand the SYSTEM tree
   6. Expand the CurrentControlSet tree
   7. Expand the Control tree
   8. Click the Lsa directory
   9. Double click nolmhash (Hopefully it is there)
   10. Change the value from “0” to “1”

2)Check Password Requirements:

1. Click the start button
2. Go to programs
3. Go to administrative tools
4. Click local security settings
5. Click account policies
6. Make sure “Enforce Password History” has 0 passwords remembered
7. Change minimum password length to not be on (THIS IS EXPLOITABLE IF ON)
8. Change passwords must meet complexity requirements (THIS IS EXPLOITABLE IF ENABLED)
9. Make sure to DISABLE “Store password using reversible encryption for all users in the domain (LEAVE THIS WINDOW OPEN YOU WILL BE RETURNING TO IT AFTER CHANGING YOUR PASSWORD AND HANDLING USERS)

3) Changing Administrator password and handle users

1. Click start
2. Go to programs
3. Go to administrative tools
4. Click Computer management
5. Click Local Users and Groups
6. Double Click Users
7. Find your administrator account (There should only be 1)
   1. IF there are OTHER administrator accounts right click THEM
   2. Click properties
   3. Click the “Member Of” tab
   4. Click the “Administrators” group
   5. Click the “Remove” button
   6. Click the “Apply” button
   7. Click back to the “General” tab
   8. Click the “Account is disabled” checkbox
   9. Repeat for any other administrator accounts
8. Right click your administrator account
9. Click “Set Password”
10. Change the password to your desired password
11. 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

4) Firewall

1. Click start
2. Go to settings
3. Go to Control Panel
4. Right click “Network and Dial-Up Connections”
5. Click “Open”
6. Right click the interface/network you want to secure (this should be all of them one by one)
7. Click “Properties”
8. Click “Internet Protocol (TCP/IP)”
9. Click “Properties”
10. Click the “Advanced” button
11. Click the “Options” Tab
12. Click “TCP/IP Filtering”
13. Click the “Properties” button
14. Click the “Enable TCP/IP Filtering (All adapters)” checkbox
15. Click the “Permit Only” radio button
16. Add the desired ports on the desired connection types

5) 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

6) Account Lockout/Audits (IF YOU HAVE TIME):

(GO BACK TO THE WINDOW FROM CHECK PASSWORD REQUIREMENTS WINDOW)

1. Click “Account Lockout Policy”
2. Set “Account Lockout Duration” to 1 minute (or whatever advised to)
3. Set “Account Lockout threshold” to 5
4. Set “Reset Account Lockout Counter” after 1 minute
5. Click “Local Policies”
6. Click “Audit Policy”
7. Enable ALL the audits