

# Windows XP Pro Security Recommended Checklist

## OS

- NTFS

## Components to Not install unless necessary

- Fax Services
- IIS
- MSN Explorer
- Network Monitoring Tools
- Networking Services
- Outlook Express
- Windows Messenger

## Creating Administrator Password

- Must have password
- 7+ characters
- mix of upper/lower letters, numbers & symbols
- No account with same username and password
- Do not use “password” “12345”, name, etc. as passwords

## Accounts

- All accounts must have “good” password as listed above
- Create Limited account for most work, use Runas for admin. Tasks
- Do not use welcome screen (picture based login) or fast user switching unless absolutely necessary

## OS Patch

- Sp1
- RPC Dcom MS03-039

## IIS Patch

- MS02-062

## L.S.P. - Account Policy (Password Policy)

- Password History = 5
- Password Length = 7 or more
- Complexity Requirements = Enabled

## L.S.P – Account Policy (Account Lockout Policy)

- Lockout Duration – 15 minutes or more
- Lockout threshold – 5 or less

- Lockout reset counter – 15 minutes or more

#### L.S.P – Local Policies (Audit Policy)

- Account Logon Events – Success / Failure
- Account Management – Success / Failure
- Directory Service Access – Failure
- Logon Events – Success / Failure
- Object Access – If you want to audit this, S/F
- Policy change – Success / Failure
- Privilege Use – Failure
- Process Tracking – Failure
- System Events – Failure

#### L.S.P. – Local Policies (User Rights Assignment)

- Access this computer from the network – remove “everyone”

#### L.S.P. – Local Policies (Security Options)

- Accounts: Guest Account Status – disabled
- Accounts: Rename Administrator account – please do this!
- Accounts: Rename Guest account – please do this!
- Accounts: Limit local use of blank passwords to console logon – DO NOT change this to disabled!
- Devices: Restrict CD-ROM and Floppy to locally logged on user – Enabled
- Interactive Logon: Do not display last user name in logon screen – Enabled
- Interactive Logon: Message text and Message Title for users attempting to log on – Whatever you want this to say
- Network Access: Do not allow anonymous enumeration of SAM Accounts – Enabled
- Network Access: Do not allow anonymous enumeration of SAM Account and Shares – Enabled
- Network Access: Remotely accessible registry paths: remove all paths
- Shutdown: Allow system to be shut down without having to log on – Disabled
- Shutdown – Clear virtual memory pagefile when shutting down - Enabled

#### Services to Disable

- Remote Registry
- Remote Desktop Help Session Manager
- Remote Access Auto Connection Manager
- Netmeeting Remote Desktop Sharing
- SSDP (Universal Plug and Play)

### Built-in Applications to disable

- Remote Assistance
- Remote Desktop
- Network folder and printer searching

### Applications to Install / Run

- Antivirus product
- Personal Firewall (ICF, ZoneAlarm, Symantec, Tiny)
- Baseline Security Analyzer
- Netstat -na
- Fport or TCPView
- Chkdsk /f