IMPORTANT
- **System Updates:**
  - Check for updates: ` `
  - Install updates: Since Server 2008 lacks a direct PowerShell command for installing updates, use the GUI or download specific patches from the Microsoft Update Catalog.

gpedit.msc

- **Change Default Passwords:**
  - Change a user's password: `net user [username] [newpassword]`

User Permissions
- **Configure UAC to Always Notify:**
  - PowerShell does not provide a direct method to change UAC settings. This needs to be changed through the Control Panel or by editing the registry: `Set-ItemProperty -Path HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\System -Name EnableLUA -Value 1`

- **Disable Guest Account:**
  - `net user guest /active:no`

Updates
- **Enable Automatic Updates:**
  - Automatic updates can be configured through the GUI in Windows Server 2008. For Server Core or automation, you might need to manipulate registry keys or use `sconfig`.

Firewalls
- **Enable and Configure Windows Firewall:**
  - Enable Firewall: `netsh advfirewall set allprofiles state on`
  - Add Firewall Rule: `New-NetFirewallRule -DisplayName "Allow 80" -Direction Inbound -Protocol TCP -LocalPort 80 -Action Allow`

Disable unused ports:

- `Wf.msc`
- `Check open ports netstat -an | Select-String 3389`
- `netstat -abno`

Windows Features and Programs
- **Uninstall Suspicious Programs:**
  - Uninstalling programs typically requires GUI interaction through `appwiz.cpl`. For automated removals, you might need to use Windows Installer commands or third-party tools.

Services

- **Manage Services:**
  - Stop a service: `Stop-Service -Name [ServiceName]`
  - Disable a service: `Set-Service -Name [ServiceName] -StartupType Disabled`

Remote Access
- **Configure Remote Settings:**
  - Disable Remote Desktop: `Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server' -name "fDenyTSConnections" -value 1`

Group Policy and Security Policy
- **Configure GPO and Security Policies:**
  - Group Policy commands typically require changes through the Group Policy Editor (`gpedit.msc`). However, you can use `secedit` for some settings:
    - Export Security Settings: `secedit /export /cfg c:\secconfig.cfg`
    - Import Security Settings: `secedit /configure /db %windir%\security\local.sdb /cfg c:\secconfig.cfg /areas SECURITYPOLICY`

Disable PowerShell for Non-Administrators
- **Restrict PowerShell Usage:**
  - This is more complex and involves setting NTFS permissions on the PowerShell executable or using AppLocker, which is not available in Windows Server 2008 by default.

Sysinternals Tools
- **Utilize Sysinternals:**
  - Access Sysinternals tools: `pushd \\live.sysinternals.com\tools`

Additional Security Considerations
- **Disable Unnecessary Protocols and Services:**
- List running Processes Get-Process
- Confirm that Processes are running at trusted paths

Get-WmiObject Win32_Process | Where-Object { $_.Name -match "svchost|lsass|smss|csrss|wininit|services" } | Select-Object Name, ExecutablePath | Format-Table -AutoSize

  - Disable Telnet (if installed): `sc config TlntSvr start= disabled`
  - Disable Teredo Tunneling: `netsh interface teredo set state disabled`

Network Egress Control
- **Configure Outbound Firewall Rules:**
  - To restrict outbound connections, you'll need to create outbound rules in the Windows Firewall:
    - `New-NetFirewallRule -DisplayName "Block Outbound" -Direction Outbound -Action Block`