

Windows Server Guide with Commands

This guide provides step-by-step instructions and commands for securing and managing Windows Server during a CyberPatriot competition.

1. User Account Management

- List all users:

Command: ``net user``

- Remove unnecessary users:

Command: ``net user username /delete``

- Reset a user's password:

Command: ``net user username newpassword``

- Disable a user account:

Command: ``net user username /active:no``

- Enable a user account:

Command: ``net user username /active:yes``

2. Group Policy Settings

- Open Group Policy Editor:

Command: ``gpedit.msc``

- Set password policies:

Path: ``Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy``

Configure:

- Enforce password history: 24
- Minimum password length: 8 characters

- Password must meet complexity requirements: Enabled
- Enable audit policies:
Path: `Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy`

Configure:

- Audit account logon events: Success, Failure
- Audit logon events: Success, Failure
- Audit object access: Success, Failure

3. Windows Firewall Configuration

- Open Windows Firewall settings:

Command: `wf.msc`

- Enable or disable the firewall:

Command: `netsh advfirewall set allprofiles state on` (to enable)

Command: `netsh advfirewall set allprofiles state off` (to disable)

- Add a rule to allow specific traffic:

Command: `netsh advfirewall firewall add rule name="RuleName" dir=in action=allow protocol=TCP localport=80`

- Block specific traffic:

Command: `netsh advfirewall firewall add rule name="BlockRule" dir=in action=block protocol=TCP localport=23`

4. Service Management

- List all services:

Command: `sc query`

- Stop a service:

Command: `net stop ServiceName`

- Disable a service:

Command: ``sc config ServiceName start= disabled``

- Start a service:

Command: ``net start ServiceName``

5. Windows Updates

- Check for updates via PowerShell:

Command: ``Install-Module PSWindowsUpdate``

Command: ``Get-WindowsUpdate``

- Install updates:

Command: ``Install-WindowsUpdate -AcceptAll -AutoReboot``

6. File and Folder Permissions

- View permissions for a file or folder:

Command: ``icacls "C:\path\to\file_or_folder"``

- Grant permissions:

Command: ``icacls "C:\path\to\file_or_folder" /grant username:F``

- Remove permissions:

Command: ``icacls "C:\path\to\file_or_folder" /remove username``

Final Notes

- Always document changes made to the system.
- Ensure all tasks are completed as per the competition checklist.
- Save all configurations and verify settings before submission.