Making Backup Admin Account

CMD

net user <name> * /ADD

net localgroup administrators <name> /add

User Management

CMD

net user

net user /domain

net user <username>

net user <username> /domain

PowerShell

Get-LocalUser

Get-ADUser -Filter *

Get-ADUser <username> -Properties *

Add/Delete Users

CMD

net user <username> <password> /add

net user <username> /del

PowerShell

New-LocalUser "<username>" -Password (ConvertTo-SecureString "<password>" -AsPlainText -Force)

Remove-LocalUser -Name "<username>"

Change Password

CMD

net user <username> N3wP@$$w0rd

PowerShell

Set-LocalUser -Name "<username>" -Password (ConvertTo-SecureString "N3wP@$$w0rd" -AsPlainText -Force)

Administrator Group Management

CMD

net localgroup administrators

PowerShell

Get-LocalGroupMember -Group "Administrators"

Create File

You can create a file with the notepad command. If it is a .exe file use .*filename* to start the program and if it is a .ps1 file use the powershell -File *filename* command to run it.

notepad *filename*

.*filename*

powershell -File *filename*

Add / Remove Administrator

CMD

net localgroup administrators <username> /add

net localgroup administrators <username> /del

PowerShell

Add-LocalGroupMember -Group "Administrators" -Member "<username>"

Remove-LocalGroupMember -Group "Administrators" -Member "<username>"

Password Policy

CMD

net accounts /minpwlen:10 /maxpwage:90 /minpwage:5 /uniquepw:10

PowerShell (View Domain Policy)

Get-ADDefaultDomainPasswordPolicy

Account Lockout Policy

CMD

net accounts /lockoutthreshold:5 /lockoutduration:30 /lockoutwindow:30

PowerShell

Start-Process cmd -ArgumentList "/c net accounts /lockoutthreshold:5 /lockoutduration:30 /lockoutwindow:30" -NoNewWindow -Wait

---

Firewall

CMD

netsh advfirewall set allprofiles state on

netsh advfirewall set allprofiles firewallpolicy blockinbound,allowoutbound

PowerShell

Start-Process netsh -ArgumentList "advfirewall set allprofiles state on","advfirewall set allprofiles firewallpolicy blockinbound,allowoutbound" -NoNewWindow -Wait

---

Windows Update

CMD

sc config wuauserv start= auto

sc start wuauserv

PowerShell

Get-Service wuauserv

sc config wuauserv start= auto | Start-Service wuauserv

Windows Defender

CMD

sc config WinDefend start= auto

sc start WinDefend

PowerShell

Get-MpPreference | Select DisableRealtimeMonitoring

Set-MpPreference -DisableRealtimeMonitoring $false

Scheduled Tasks

CMD

schtasks /delete /tn * /f

SMB Shares

CMD

net share

net share <sharename> /delete

Flushing DNS Cache and Checking Cache

CMD

ipconfig /flushdns

cmdkey /list

Threat Hunting / Incident Response

Remove File Types

CMD

for /r C:\ %i in (*.mp3) do del /f /q “%i”

PowerShell

Get-ChildItem -Path C:\ -Recurse -Filter *.mp3

Get-ChildItem -Path C:\ -Recurse -Filter *.mp3 | Remove-Item -Force

---

Remove Network Share

CMD

net share <sharename> /del

PowerShell

Remove-SmbShare -Name "<sharename>"

Running Processes

CMD

tasklist

tasklist | findstr "badguy"

wmic service list brief | findstr "Running"

wmic service list full

sc stop <serviceName>

PowerShell

Get-Process

Get-Process | Select ID, ProcessName, Path

Get-Process | Select-String "badguy"

Stop-Process -Name "badguy"

Remove Software

CMD

wmic product where "name like '<software_name>'" call uninstall

PowerShell

Get-WmiObject -Query "SELECT * FROM Win32_Product WHERE Name LIKE '%<software_name>%'" | ForEach-Object {

$_.Uninstall()

}

Disable Malicious Service

CMD

sc config ftpsvc start= disabled

net stop ftpsvc

PowerShell

Set-Service -Name "FTPSVC" -StartupType Disabled

Stop-Service -Name "FTPSVC"

Configure AD Group Policy

Network Security Settings

Configure in Local Security Policy (secpol.msc) or GPO.

Access:

Win+R → secpol.msc / Win+R → gpedit.msc

Location:

Security Settings

→ Local Policies

→ Security Options

- **Network security: LAN Manager authentication level**
  → Send NTLMv2 response only; refuse LM & NTLM
- **Network security: Do not store LAN Manager hash value on next password change**
  → Enabled

Anonymous Access Restrictions

- **Network access: Do not allow anonymous enumeration of SAM accounts and shares**
  → Enabled
- **Network access: Do not allow anonymous enumeration of SAM accounts**
  → Enabled
- **Network access: Allow anonymous SID/name translation**
  → Disabled

Account Security

- **Accounts: Rename administrator account**
  → Rename to something unique (and document it)

Interactive Logon

- **Interactive logon: Message text for users attempting to log on**
  → Configure login banner (sometimes required in CCDC injects)

Scripts

remove-python.ps1

Get-CimInstance Win32_Product |

Where-Object Name -like "Python*" |

Invoke-CimMethod -MethodName Uninstall

Auditing Configuration

Enable auditing for both **Success and Failure** where listed.

Audit Policies

- Audit process tracking → **Success**
- Audit account management → **Success, Failure**
- Audit logon events → **Success, Failure**
- Audit account logon events → **Success, Failure**
- Audit object access → **Success, Failure**

Location:

Local Policies → Audit Policy

Account Lockout Policy (GPO or Local Policy)

Location:

Security Settings → Account Policies → Account Lockout Policy

Recommended competition settings:

- Account Lockout Duration → **30 minutes**
- Account Lockout Threshold → **2 failed logins**
- Reset account lockout counter after → **30 minutes**

Require AES-128 (prevent Netlogon / legacy crypto abuse)

Win+R → gpmc.msc

Default Domain Controllers Policy

Create GPO

→ Computer Configuration

→ Policies

→ Windows Settings

→ Security Settings

→ Local Policies

→ Security Options

Network security: Configure encryption types allowed for Kerberos

Select:

AES128_HMAC_SHA1

AES256_HMAC_SHA1

Uncheck:

DES

RC4

OR

```
New-Item "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT" -Name DNSClient -Force
New-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient" -Name EnableMultiCast -Value 0 -PropertyType DWORD -Force
New-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient" -Name DisableSmartNameResolution -Value 1 -PropertyType DWORD -Force
```

Get autologon, Sysmon, autoruns

Group Policy Tasks

Create GPO: Account Lockout

Configure:

- Lockout threshold
- Lockout duration
- Reset timer

Create GPO: PowerShell Logging

Enable:

- Verbose PowerShell logging
- PowerShell transcription logging

Tool Reference

Open Local Security Policy:

secpol.msc

Download Malwarebytes!

Disable IPv6

1. **Open Settings.**
2. **Click on Network & internet.**
3. **Click the Advanced network settings option.**
4. **Under the Related settings section, click the More network adapter options setting.**
5. **Right-click the network adapter and choose Properties.**
6. **Clear the Internet Protocol Version 6 (TCP/IPv6) option.**

Turn Off Teredo

CMD

netsh interface teredo set state disabled

DO THIS!

Enable and set to highest setting UAC

C:\windows\system32\UserAccountControlSettings.exe

Check startup & disable unnecessary items via msconfig

msconfig

Uninstall any unnecessary software

Control appwiz.cpl

Forces Netlogon communication to be encrypted when computers talk to a Domain Controller

Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters" -Name "RequireSeal" -Value 2 -Type DWORD

Monitor

Win+R → lusrmgr.msc

Win+R → eventvwr.msc

Win+R → services.msc

taskmgr.exe

Event IDs

5379 — Attempted to read stored credentials

4624 — Successful login

4625 — Failed login

4720 — User created

4732 — Added to administrators

4688 — Process created

4672 — Admin login

1102 — Log cleared