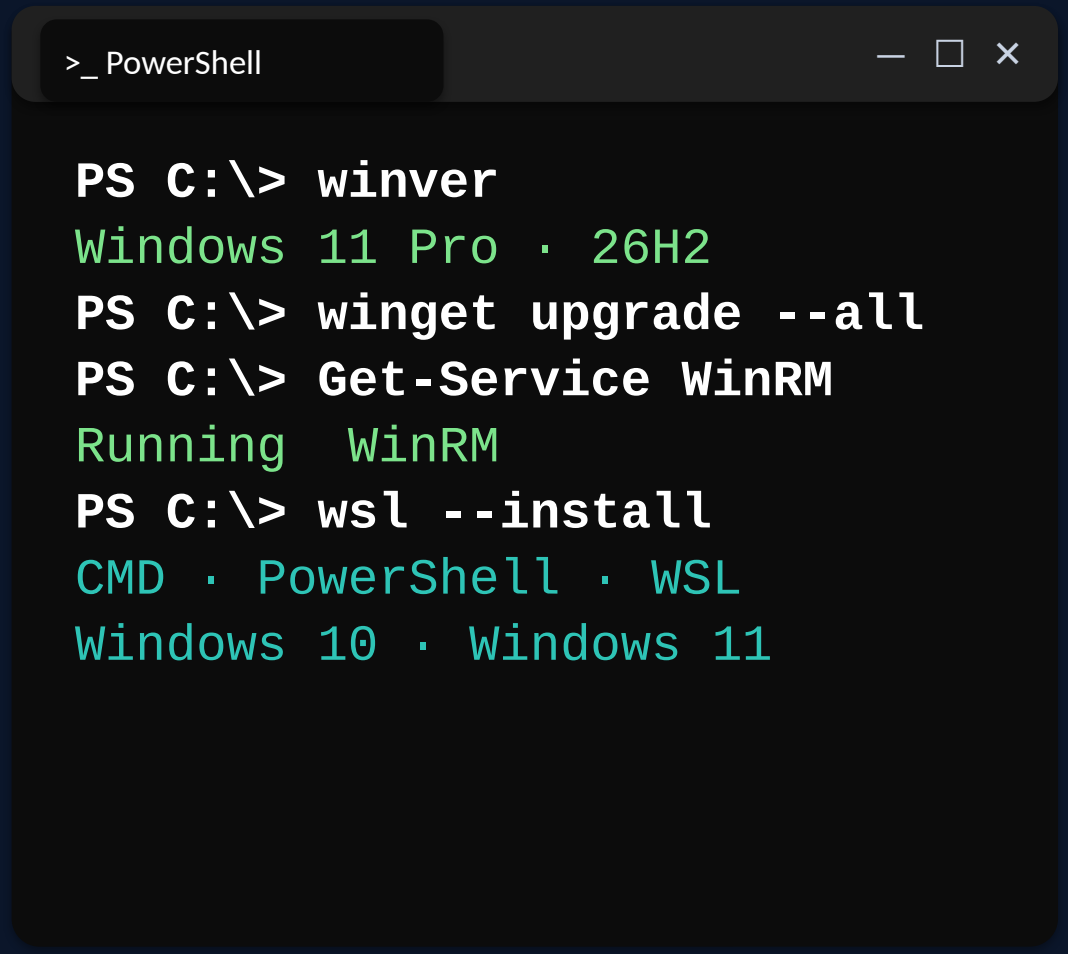


LESSON 9 OF 12

Windows 10 & 11

Desktop · Workstation · Laptop

Processes, Services, Scheduled Tasks & Event Logs

Full Course · Windows 11 26H2 · Windows 10 22H2

What You Will Learn in Lesson 9

- Processes, threads, PIDs and svchost.exe
- Listing and stopping processes: tasklist, taskkill, Get-Process
- Services: startup types, accounts, dependencies and recovery
- Everything that starts automatically, and how to control it
- Task Scheduler: run jobs on a schedule or at an event
- Event Viewer and Get-WinEvent: reading the logs like a detective
- Sysinternals: Process Explorer, Autoruns and Process Monitor

Processes: The Basics

Term	Meaning
Process	A running program with its own memory, e.g. notepad.exe
Thread	A path of execution inside a process; processes have one or many
PID	Process ID, a number that identifies the process right now
Session 0	Where services run, separate from users' desktops
svchost.exe	A host that runs one or more Windows services
Elevated	Running with full administrator rights (after UAC)

Processes with CMD

```
C:\> tasklist                                    # every process, PID, memory
C:\> tasklist /svc /fi "imagename eq svchost.exe" # which services each svchost runs
C:\> tasklist /fi "memusage gt 500000"           # using more than ~500 MB
C:\> start notepad
C:\> taskkill /im notepad.exe                     # ask it to close
C:\> taskkill /im notepad.exe /f                  # force
C:\> taskkill /pid 4321 /t /f                     # a PID and its child processes
```

Processes with PowerShell

```
PS C:\> Get-Process | Sort-Object WS -Descending | Select-Object -First 8 Name, Id,
          @{n='MemMB'; e={[int]($_.WS / 1MB)}}, CPU

PS C:\> $p = Start-Process notepad -PassThru ; $p.Id
PS C:\> Stop-Process -Id $p.Id
PS C:\> Get-Process chrome -ErrorAction SilentlyContinue | Stop-Process -WhatIf

PS C:\> Get-CimInstance Win32_Process -Filter "Name='pwsh.exe'" |
          Select-Object ProcessId, ParentProcessId, CommandLine
```

Services: What to Know

Setting	Options and meaning
Startup type	Automatic, Automatic (Delayed Start), Manual, Disabled
Trigger start	Starts when an event happens, e.g. a USB device or network
Log on as	LocalSystem (most powerful), LocalService, NetworkService, a user
Dependencies	Services that must run first — check before stopping
Recovery	What to do on failure: restart the service, run a program
Golden rule	Do not disable services you do not understand

Services with sc and PowerShell

```
C:\> sc query wuauserv                    # Windows Update service state
C:\> sc qc Spooler                        # configuration: start type, account

PS C:\> Get-Service | Where-Object Status -eq Running | Measure-Object
PS C:\> Get-Service Spooler | Select-Object Name, Status, StartType, DependentServices
PS C:\> Restart-Service Spooler                       # fix a stuck print queue
PS C:\> Set-Service Spooler -StartupType Manual       # run as Administrator
PS C:\> Get-CimInstance Win32_Service | Where-Object StartName -like '*LocalSystem*' |
            Select-Object -First 5 Name, StartMode, PathName
```

Everything That Starts Automatically

Location	How to manage it
Startup apps	Settings > Apps > Startup, or Task Manager > Startup apps
Startup folders	shell:startup (you) and shell:common startup (everyone)
Run registry keys	HKCU / HKLM \Software\Microsoft\Windows\CurrentVersion\Run
Scheduled tasks	taskschd.msc — many apps add update tasks here
Services and drivers	services.msc, Device Manager
See it all at once	Sysinternals Autoruns

Task Scheduler from the Command Line

```
C:\> schtasks /query /fo table | more
C:\> schtasks /create /tn "LabBackup" /sc daily /st 22:00 ^
      /tr "robocopy C:\Lab D:\Backup\Lab /E /R:1 /W:1"

PS C:\> $a = New-ScheduledTaskAction -Execute 'pwsh.exe' -Argument '-File C:\Lab\backup.ps1'
PS C:\> $t = New-ScheduledTaskTrigger -Daily -At 10pm
PS C:\> Register-ScheduledTask -TaskName 'LabBackupPS' -Action $a -Trigger $t
PS C:\> Start-ScheduledTask -TaskName 'LabBackupPS'
PS C:\> Get-ScheduledTaskInfo -TaskName 'LabBackupPS'    # LastRunTime, LastTaskResult
```

Event Logs: Where Windows Writes Everything

Event ID	Log	Meaning
41	System (Kernel-Power)	Restarted without a clean shutdown (crash, power loss)
1074	System	Who or what started a shutdown or restart
6005 / 6006	System	Event Log service started / stopped (boot / shutdown)
7036 / 7034	System	A service changed state / stopped unexpectedly
1000	Application	An application crashed
4624 / 4625	Security	Successful / failed sign-in

Reading Logs with PowerShell

```
PS C:\> Get-WinEvent -LogName System -MaxEvents 10 | Format-Table TimeCreated, Id, LevelDisplayName, Message -Wrap

PS C:\> Get-WinEvent -FilterHashtable @{LogName='System'; Id=41,1074,6008} -MaxEvents 20

PS C:\> Get-WinEvent -FilterHashtable @{LogName='Application'; Level=2; StartTime=(Get-Date).AddDays(-7)}

PS C:\> Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4625} -MaxEvents 10   # admin

C:\> wevtutil qe System /c:5 /rd:true /f:text      # CMD alternative
```

Sysinternals: The Pro Toolkit (Free)

- Process Explorer: Task Manager on steroids; check processes with VirusTotal
- Autoruns: every auto-start location; uncheck to disable safely
- Process Monitor: live file, registry and process activity
- TCPView: which process has which network connection
- Get them: learn.microsoft.com/sysinternals or the Microsoft Store
- Also: PsExec, Sysmon, RAMMap, Disk2vhd

Lab: Be the Detective

```
PS C:\> Get-Process | Sort-Object CPU -Descending | Select-Object -First 5 Name, Id, CPU
PS C:\> Get-Service | Where-Object {$_.StartType -eq 'Automatic' -and $_.Status -ne 'Running'}
PS C:\> Get-WinEvent -FilterHashtable @{LogName='System'; Id=41,6008} -MaxEvents 5
PS C:\> Get-WinEvent -FilterHashtable @{LogName='System'; Id=6005} -MaxEvents 5 |
          Select-Object TimeCreated          # your last five boots
# Create the LabBackupPS task, run it, then check:
PS C:\> Get-ScheduledTaskInfo LabBackupPS | Select-Object LastRunTime, LastTaskResult
```

Summary & Homework

- tasklist / taskkill and Get-Process / Stop-Process manage processes
- Services: know startup types and accounts; never disable blindly
- Control auto-start: Startup apps, Task Scheduler, Autoruns
- Logs: 41, 1074, 6005, 1000, 4625 — Get-WinEvent -FilterHashtable
- Homework: schedule a daily backup with Register-ScheduledTask
- Homework: use Autoruns to review everything that starts on your PC

Thank You! 🙏

Free videos & PDFs: www.MyWebUniversity.com

Slides for this lesson: MyWebUniversity.com/presentations

YouTube: @MyWebUniversity · @MyWebUniversity-Dari

Wahidullah Lutfy — Founder and Director of IT of MyWebUniversity, and CS teacher

Book: The Direct Path to Linux Ubuntu (Amazon · Barnes & Noble)

Learn it, then pass it on.