درس ۹ از ۱۲

Windows 10 & 11

Desktop · Workstation · Laptop

پروسه‌ها، سرویس‌ها، کارهای زمان‌بندی‌شده و لاگ‌ها

دوره کامل · Windows 10 22H2 · Windows 11 26H2



در درس نهم چه یاد می‌گیرید

- پروسه‌ها، thread ها، PID ها و svchost.exe
- لست و متوقف کردن پروسه‌ها: Get-Process، taskkill، tasklist
- سرویس‌ها: نوع شروع، حساب‌ها، وابستگی‌ها و بازیابی
- هر چیزی که خودکار شروع می‌شود و چگونه آن را کنترل کنیم
- Task Scheduler: اجرای کارها طبق زمان‌بندی یا با یک رویداد
- Event Viewer و Get-WinEvent: خواندن لاگ‌ها مانند یک کارآگاه
- Sysinternals: Process Explorer، Autoruns و Process Monitor

پروسه‌ها: اصول

اصطلاح	معنی
Process	یک برنامه در حال اجرا با حافظه خودش، مثلاً notepad.exe
Thread	یک مسیر اجرا داخل یک پروسه؛ پروسه‌ها یک یا چند thread دارند
PID	شماره پروسه، عددی که پروسه را همین حالا مشخص می‌کند
Session 0	جایی که سرویس‌ها اجرا می‌شوند، جدا از دسکتاپ کاربران
svchost.exe	یک میزبان که یک یا چند سرویس ویندوز را اجرا می‌کند
Elevated	اجرا با دسترسی کامل admin (بعد از UAC)

پروسه‌ها با 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
```

پروسه‌ها با 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
```

سرویس‌ها: چه چیزی بدانید

گزینه‌ها و معنی	تنظیم
Automatic، Automatic (Delayed Start)، Manual، Disabled	نوع شروع
وقتی یک رویداد اتفاق می‌افتد شروع می‌شود، مثلاً یک دستگاه USB یا شبکه	Trigger start
LocalSystem (قوی‌ترین)، NetworkService، LocalService، یک کاربر	Log on as
سرویس‌هایی که باید اول اجرا شوند — قبل از توقف بررسی کنید	وابستگی‌ها
هنگام خرابی چه کار کند: سرویس را ری‌استارت کند، یک برنامه را اجرا کند	بازیابی
سرویس‌هایی را که نمی‌فهمید غیرفعال نکنید	قانون طلایی

سرویس‌ها با sc و 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
```

هر چیزی که خودکار شروع می‌شود

محل	چگونه مدیریت کنیم
Startup apps	Settings > Apps > Startup، یا Task Manager > Startup apps
فولدرهای Startup	shell:startup (شما) و shell:common startup (همه)
کلیدهای Run در Registry	HKCU / HKLM \Software\Microsoft\Windows\CurrentVersion\Run
Scheduled tasks	taskschd.msc — بسیاری از برنامه‌ها کارهای آپدیت را این جا اضافه می‌کنند
سرویس‌ها و درایورها	services.msc، Device Manager
دیدن همه یک‌جا	Sysinternals Autoruns

Task Scheduler از خط فرمان

```
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
```

لاگ‌ها: جایی که ویندوز همه چیز را می‌نویسد

معنی	لاگ	Event ID
بدون خاموشی درست ری‌استارت شد (crash، قطع برق)	System (Kernel-Power)	41
چه کسی یا چه چیزی خاموشی یا ری‌استارت را شروع کرد	System	1074
سرویس Event Log شروع / متوقف شد (بوت / خاموشی)	System	6005 / 6006
یک سرویس وضعیت را تغییر داد / غیرمنتظره متوقف شد	System	7036 / 7034
یک برنامه crash کرد	Application	1000
ورود موفق / ناموفق	Security	4624 / 4625

خواندن لاگ‌ها با 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: جعبه ابزار حرفه‌ای (رایگان)

- Process Explorer: یک Task Manager بسیار قوی؛ بررسی پروسه‌ها با VirusTotal
- Autoruns: هر محل شروع خودکار؛ با برداشتن تیک با امنیت غیرفعال کنید
- Process Monitor: فعالیت زنده فایل، registry و پروسه
- TCPView: کدام پروسه کدام اتصال شبکه را دارد
- دریافت: learn.microsoft.com/sysinternals یا Microsoft Store
- همچنین: Disk2vhd، RAMMap، Sysmon، PsExec

لابراتوار: کارآگاه باشید

```
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
```

خلاصه و کارخانگی

- tasklist / taskkill و Get-Process / Stop-Process پروسه‌ها را مدیریت می‌کنند
- سرویس‌ها: نوع شروع و حساب‌ها را بشناسید؛ هرگز کورکورانه غیرفعال نکنید
- شروع خودکار را کنترل کنید: Autoruns، Task Scheduler، Startup apps
- لاگ‌ها: 41، 1074، 6005، 1000، 4625 — Get-WinEvent -FilterHashtable
- کارخانگی: یک بکاپ روزانه با Register-ScheduledTask زمان‌بندی کنید
- کارخانگی: با Autoruns هر چیزی را که روی کمپیوترتان شروع می‌شود بررسی کنید

تشکر از شما! 🤲

ویدیوها و PDF های رایگان: www.MyWebUniversity.com

سلایدهای این درس: MyWebUniversity.com/presentations

YouTube: @MyWebUniversity-Dari · @MyWebUniversity

وحیدالله لطفی – مؤسس و رئیس IT مای وب یونیورسیتی، و استاد علوم کامپیوتر

یاد بگیرید و به دیگران انتقال دهید