درس ۸ از ۱۲

Windows 10 & 11

Desktop · Workstation · Laptop

مدیریت حساب‌ها: کاربران، گروه‌ها، UAC و ورود

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



در درس هشتم چه یاد می‌گیرید

- انواع حساب: Microsoft، محلی، کاری یا مکتبی، domain
- کاربر عادی در برابر admin، و UAC چگونه از شما محافظت می‌کند
- مدیریت کاربران با net user، lusrmgr.msc، Settings و PowerShell
- گروه‌های داخلی و اجازه‌های آن‌ها
- گزینه‌های ورود: passkey، PIN، Windows Hello و رمز
- پروفایل کاربران، runas و پالیسی رمز
- بهترین روش‌ها برای خانواده‌ها، مکاتب و دفترها

انواع حساب‌ها

حساب	ورود با	استفاده معمول
حساب Microsoft	ایمیل + رمز / Windows Hello	کمپیوترهای خانگی؛ Store، OneDrive، بکاپ کلید BitLocker
حساب محلی	نام کاربر + رمز، فقط این کامپیوتر	لابراتوار، کمپیوترهای مشترک یا آفلاین
کاری یا مکتبی	حساب Microsoft Entra ID	سازمان‌هایی که از Microsoft 365 و Intune استفاده می‌کنند
حساب domain	Active Directory (DOMAIN\user)	شرکت‌هایی با سرورهای داخلی
Administrator داخلی	به طور پیش‌فرض غیرفعال	فقط برای بازیابی — غیرفعال بگذارید
حساب خانواده (کودک)	Microsoft Family Safety	محدودیت زمان و محتوا برای کودکان

کاربر عادی در برابر Administrator

Administrator	کاربر عادی	
بلی	بلی	اجرای برنامه‌ها، مرور، اسناد
بلی، بعد از سوال UAC	نه (رمز admin می‌خواهد)	نصب نرم‌افزار برای همه
بلی، بعد از سوال UAC	نه	تغییر تنظیمات سیستم، درایورها
بلی	نه	مدیریت کاربران دیگر
می‌تواند کل سیستم را تغییر دهد	محدود به فایل‌های همان کاربر	خطر اگر بدافزار اجرا شود

UAC چگونه از شما محافظت می‌کند

- admin ها با یک token عادی کار می‌کنند تا وقتی یک کار دسترسی بیشتر لازم داشته باشد
- سوال تأیید (admin ها): «Do you want to allow this app...?» — Yes/No
- سوال رمز (کاربران عادی): نام و رمز یک admin را تایپ کنید
- سوال‌ها روی Secure Desktop ظاهر می‌شوند که بدافزار نمی‌تواند روی آن کلیک کند
- قبل از کلیک Yes نام ناشر را بررسی کنید
- هرگز UAC را خاموش نکنید: UserAccountControlSettings.exe

کاربران و گروه‌ها با CMD (net)

```
C:\> whoami /groups | findstr /i "Administrators"      # am I an admin?
C:\> net user                                          # list local users
C:\> net user student * /add                           # * = prompt for the password
C:\> net user student                                  # details, last logon, groups
C:\> net localgroup Administrators                     # who are the admins?
C:\> net localgroup "Remote Desktop Users" student /add
C:\> net user student /active:no                       # disable the account
C:\> net user student /delete
```

کاربران و گروه‌ها با PowerShell

```
PS C:\> Get-LocalUser | Select-Object Name, Enabled, LastLogon
PS C:\> $pw = Read-Host -AsSecureString 'Password'
PS C:\> New-LocalUser -Name student -Password $pw -FullName 'Lab Student'
PS C:\> Add-LocalGroupMember -Group Users -Member student
PS C:\> Get-LocalGroupMember -Group Administrators
PS C:\> Disable-LocalUser -Name student
PS C:\> Remove-LocalUser -Name student -WhatIf

# GUI: Settings > Accounts > Other users   |   lusrmgr.msc (Pro and higher)
```

گروه‌های داخلی مهم

گروه	اعضا می‌توانند
Administrators	هر کاری روی این کمپیوتر انجام دهند
Users	برنامه‌ها را اجرا کنند و از فایل‌های خود استفاده کنند (کاربران عادی)
Remote Desktop Users	از طریق Remote Desktop وارد شوند (درس ۱۰)
Backup Operators	از فایل‌ها بکاپ بگیرند و بازیابی کنند، حتی بدون اجازه فایل
Hyper-V Administrators	ماشین‌های مجازی را بدون admin کامل بودن مدیریت کنند
Event Log Readers / Performance Log Users	لاگ‌ها را بخوانند / دیتای performance جمع کنند

گزینه‌های ورود

گزینه	نکات
Windows Hello PIN	به این دستگاه و TPM آن بسته است — امن‌تر از یک رمز تکراری
چهره / اثر انگشت	بیومتریک Windows Hello روی کمره‌ها و خواننده‌های پشتیبانی‌شده
Passkey ها	ورود مقاوم در برابر phishing به وب‌سایت‌ها، ذخیره‌شده توسط Windows Hello
Security key	یک کلید FIDO2 از نوع USB یا NFC
رمز	هنوز در بعضی موارد لازم است؛ از جمله‌های رمز طولانی استفاده کنید
Dynamic lock	وقتی موبایل جفت‌شده شما دور می‌شود کمپیوتر را قفل می‌کند

پروفایل‌ها، runas و پالیسی رمز

```
PS C:\> Get-CimInstance Win32_UserProfile | Select-Object LocalPath, LastUseTime
# Delete old profiles: sysdm.cpl > Advanced > User Profiles > Settings

C:\> runas /user:%COMPUTERNAME%\admin2 "mmc compmgmt.msc"   # run as another user

C:\> net accounts                          # password and lockout policy
C:\> net accounts /minpwlen:12 /lockoutthreshold:10
C:\> secpol.msc                            # Local Security Policy (Pro and higher)
```

بهترین روش‌ها

- هر روز از حساب عادی استفاده کنید؛ یک حساب admin جداگانه نگه دارید
- هر نفر حساب خودش را می‌گیرد — هرگز یک حساب را شریک نکنید
- جمله‌های رمز طولانی و منحصربه‌فرد به اضافه Windows Hello؛ کدهای بازیابی را ذخیره کنید
- حساب‌هایی را که دیگر استفاده نمی‌شوند حذف یا غیرفعال کنید
- خانواده‌ها: حساب کودک با Microsoft Family Safety
- سازمان‌ها: Windows LAPS رمزهای admin محلی را خودکار عوض می‌کند

لابراتوار: کمترین دسترسی در عمل

```
PS C:\> $pw = Read-Host -AsSecureString
PS C:\> New-LocalUser labuser -Password $pw ; Add-LocalGroupMember Users labuser
# Sign out, sign in as labuser, then try:
#   - install an app for all users  -> UAC credential prompt
#   - open C:\Windows\System32 and create a file -> Access denied
C:\> whoami /groups
C:\> whoami /priv
# Back as admin: add labuser to 'Remote Desktop Users', then disable the account
PS C:\> Disable-LocalUser labuser
```

خلاصه و کارخانگی

- حساب‌های Microsoft، محلی، کاری/مکتبی و domain نیازهای متفاوت را پوشش می‌دهند
- کاربر عادی روزانه + UAC = خسارت بسیار کمتر از اشتباهات و بدافزار
- net user / net localgroup و cmdlet های *-LocalGroupMember / *-LocalUser
- PIN ویندوز Hello و passkey بهتر از رمزهای تکراری هستند
- کارخانگی: کمپیوتر خود را بررسی کنید — کاربران و گروه Administrators را لست کنید
- کارخانگی: کار روزانه خود را به یک حساب عادی منتقل 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