SYSTEMES D’EXPLOITATION
Labo 2 – Windows serveur

SOLUTION

1 Exercice 2 – Renommer votre serveur

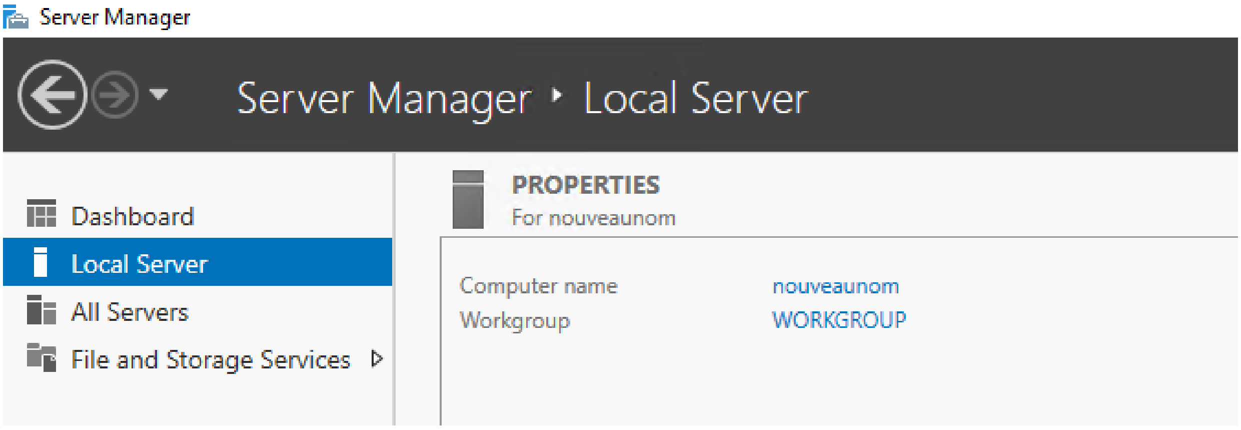
```
PS C:\Users\Administrator> get-help

        Do you want to run Update-Help?

        The Update-Help cmdlet downloads the most current Help files for Windows PowerShell
        modules, and installs them on your computer. For more information about the Update-Help
        cmdlet, see https:/go.microsoft.com/fwlink/?LinkId=210614.

        &Yes  &No  &Suspend

        N

PS C:\Users\Administrator> Get-ComputerInfo

PS C:\Users\Administrator> Get-ComputerInfo -Property CsName

PS C:\Users\Administrator> get-verb

PS C:\Users\Administrator> get-command rename*
```

FYI only

```
PS C:\Users\Administrator> get-command rename* | where {$psitem.name -match "computer"}
```

```
PS C:\Users\Administrator> get-help rename-computer
```

>> redmarrez la machine (**shutdown /r /t 0**)



Computer name nouveaunom

Workgroup WORKGROUP

2 Exercice 3 – gestion des comptes utilisateurs et des groups

```
PS C:\Users\Administrator> get-command *group*
```

```
PS C:\Users\Administrator> help New-LocalGroup
PS C:\Users\Administrator> New-LocalGroup -Name "student" -Description "Groupe etudiants"
PS C:\Users\Administrator> New-LocalGroup -Name "Whitehat" -Description "Groupe pentesters"
PS C:\Users\Administrator> Get-LocalGroup
```

Fyi only

```
    PS C:\Users\Administrator> Get-LocalGroup -Name Student, whitehat
```

```
PS C:\Users\Administrator> get-command *user*
PS C:\Users\Administrator> help New-LocalUser
PS C:\Users\Administrator> $mot_de_passe = read-host -AsSecureString
PS C:\Users\Administrator> New-LocalUser -Name "P200016" -Password $mot_de_passe -AccountNeverExpires -Description "mon user" -FullName "Olivier Masit" -PasswordNeverExpires
PS C:\Users\Administrator> get-command *group*
```

Fyi only

```
    PS C:\Users\Administrator> get-command *group* | where{$_.name -match "groupmember"}
```

```
PS C:\Users\Administrator> help add-localgroupmember
PS C:\Users\Administrator> Add-LocalGroupMember -Group "student" -Member "P200016"
PS C:\Users\Administrator> Add-LocalGroupMember -Group "administrators" -Member "P200016"
PS C:\Users\Administrator> Get-LocalGroupMember -Group "student"
PS C:\Users\Administrator> Get-LocalGroupMember -Group "student"
```

Fyi only (si ils se sont trompés 😉)

```
    PS C:\Users\Administrator> get-command *localuser*
    PS C:\Users\Administrator> help Set-LocalUser
    PS C:\Users\Administrator> help Set-LocalUser
    PS C:\Users\Administrator> Get-LocalUser -Name P200016 | Select-Object -Property *
```

Loogout / login as E…

Fyi only (un autre moyen de passer une secure string)

```
PS C:\Users\Administrator> $password = ConvertTo-SecureString -String "P@ssw0rd." -AsPlainText -Force
```

```
PS C:\Users\Administrator> New-LocalUser -Name "hacker" -Password $password -Description "pentester" -FullName "Kevin Mitnick" -AccountExpires 24/12/2020
```

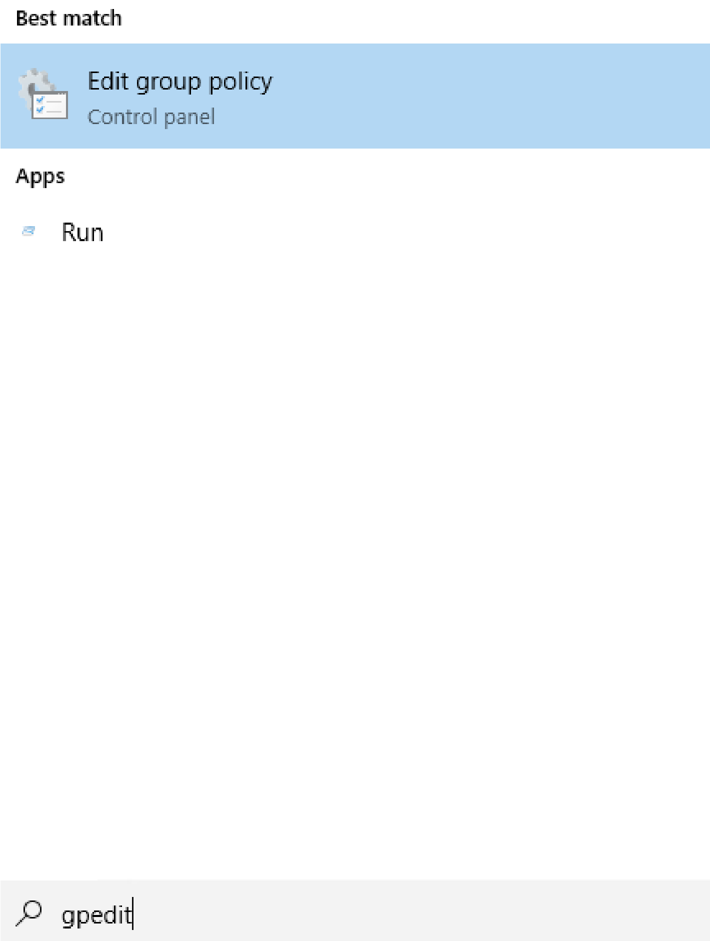
```
PS C:\Users\Administrator> Add-LocalGroupMember -Group "whitehat" -Member "hacker"
```

FYI Verif

```
Get-LocalUser "hacker" | Select-Object -Property *
```

```
>>> AccountExpires        : 24-12-20 00:00:00
```

Modifier la security policy (bcp trop compliqué en Powershell pour eux)



Best match

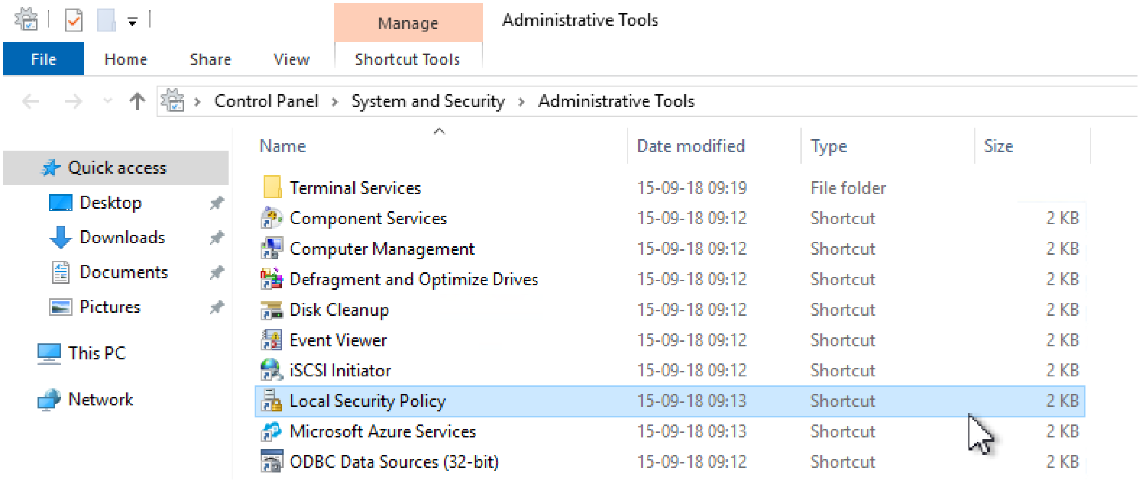
Edit group policy
Control panel

Apps

Run

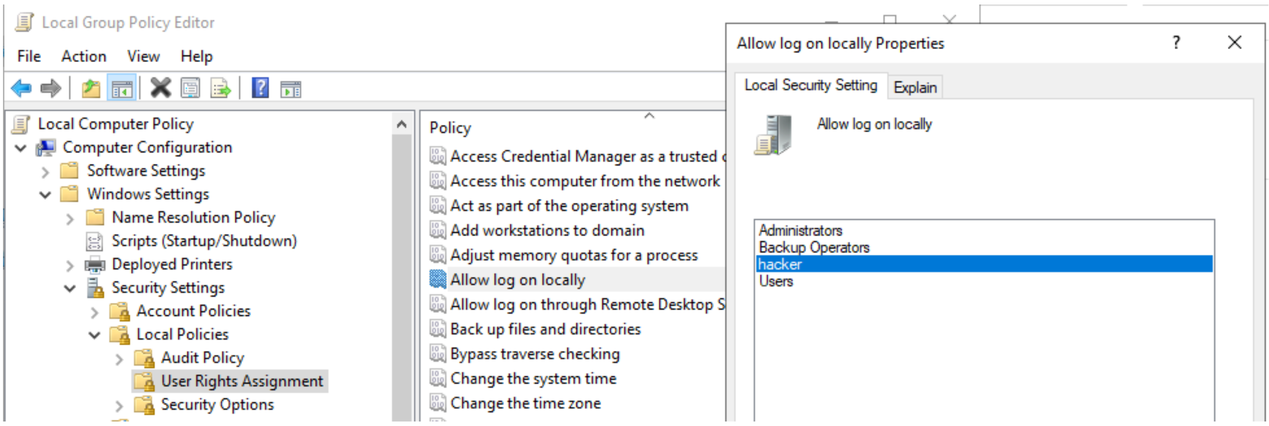
gpedit

OU



Name	Date modified	Type	Size
Terminal Services	15-09-18 09:19	File folder	
Component Services	15-09-18 09:12	Shortcut	2 KB
Computer Management	15-09-18 09:12	Shortcut	2 KB
Defragment and Optimize Drives	15-09-18 09:12	Shortcut	2 KB
Disk Cleanup	15-09-18 09:12	Shortcut	2 KB
Event Viewer	15-09-18 09:12	Shortcut	2 KB
iSCSI Initiator	15-09-18 09:12	Shortcut	2 KB
Local Security Policy	15-09-18 09:13	Shortcut	2 KB
Microsoft Azure Services	15-09-18 09:13	Shortcut	2 KB
ODBC Data Sources (32-bit)	15-09-18 09:12	Shortcut	2 KB

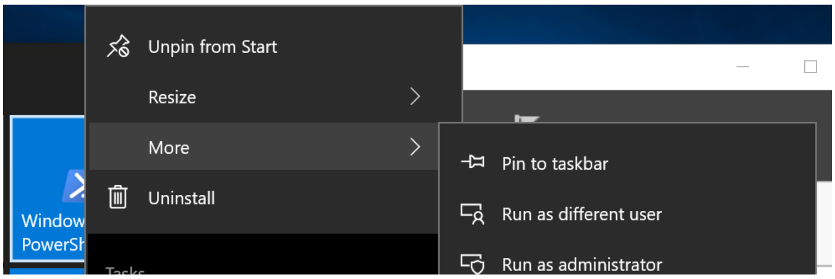
Ajouter une permission à Hacker (allow log on locally)

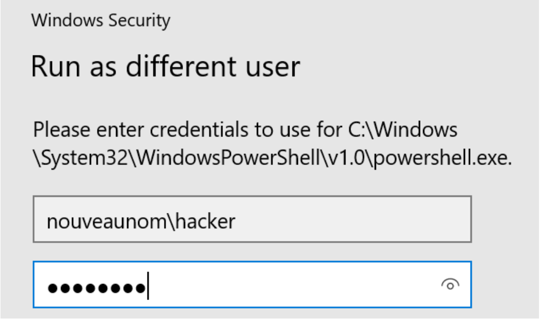


Allow log on locally

Administrators
Backup Operators
hacker
Users

Ouvrir la session PowerShell en tant que Hacker



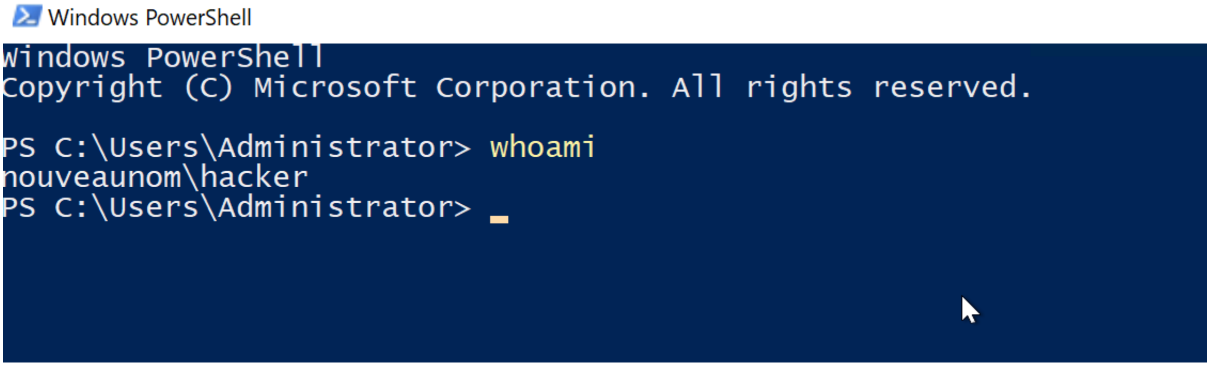

Windows Security

Run as different user

Please enter credentials to use for C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.

nouveaunom\hacker

••••••••


Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> whoami
nouveaunom\hacker
PS C:\Users\Administrator> _
```

N’hésitez pas à revenir vers moi en cas de souci.