

Administration Windows Client

PACE Fabio



TP 2

TP 2 : La boîte à outils Windows

1. Manipuler les différents outils (voir plus)
2. Créer un package MMC sur le bureau (raccourcit) contenant les outils dont vous jugez intéressant
3. Capture d'écran comprenant :
 - Une CMD avec le nom du PC (nom de l'élève)
 - Le contenu de votre MMC avec un explicatif (bref) du choix des outils

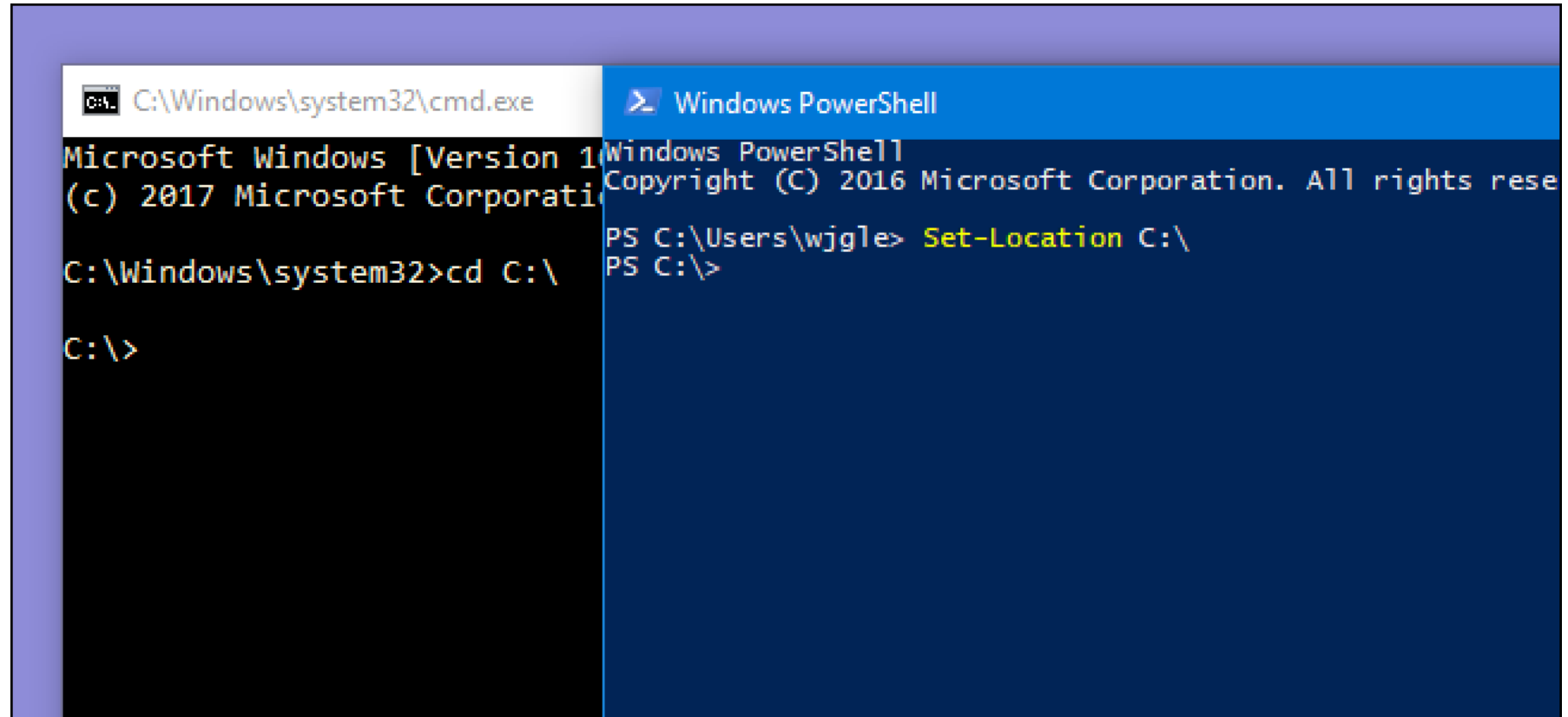
Durée maximale : 1h

Dépôt du compte rendu sur Moodle (TP 2)



POWERSHELL

Qu'est-ce que c'est ?



The image shows a side-by-side comparison of two Windows command-line interfaces. On the left is the Command Prompt (cmd.exe), and on the right is Windows PowerShell. Both windows show the user navigating to the root of the C: drive.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17134.1]
(c) 2017 Microsoft Corporation. All rights reserved.
C:\Windows\system32>cd C:\
C:\>

Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\wjgle> Set-Location C:\
PS C:\>
```



PowerShell

L'invite de commande ?

Starting MS-DOS...

C:\>_

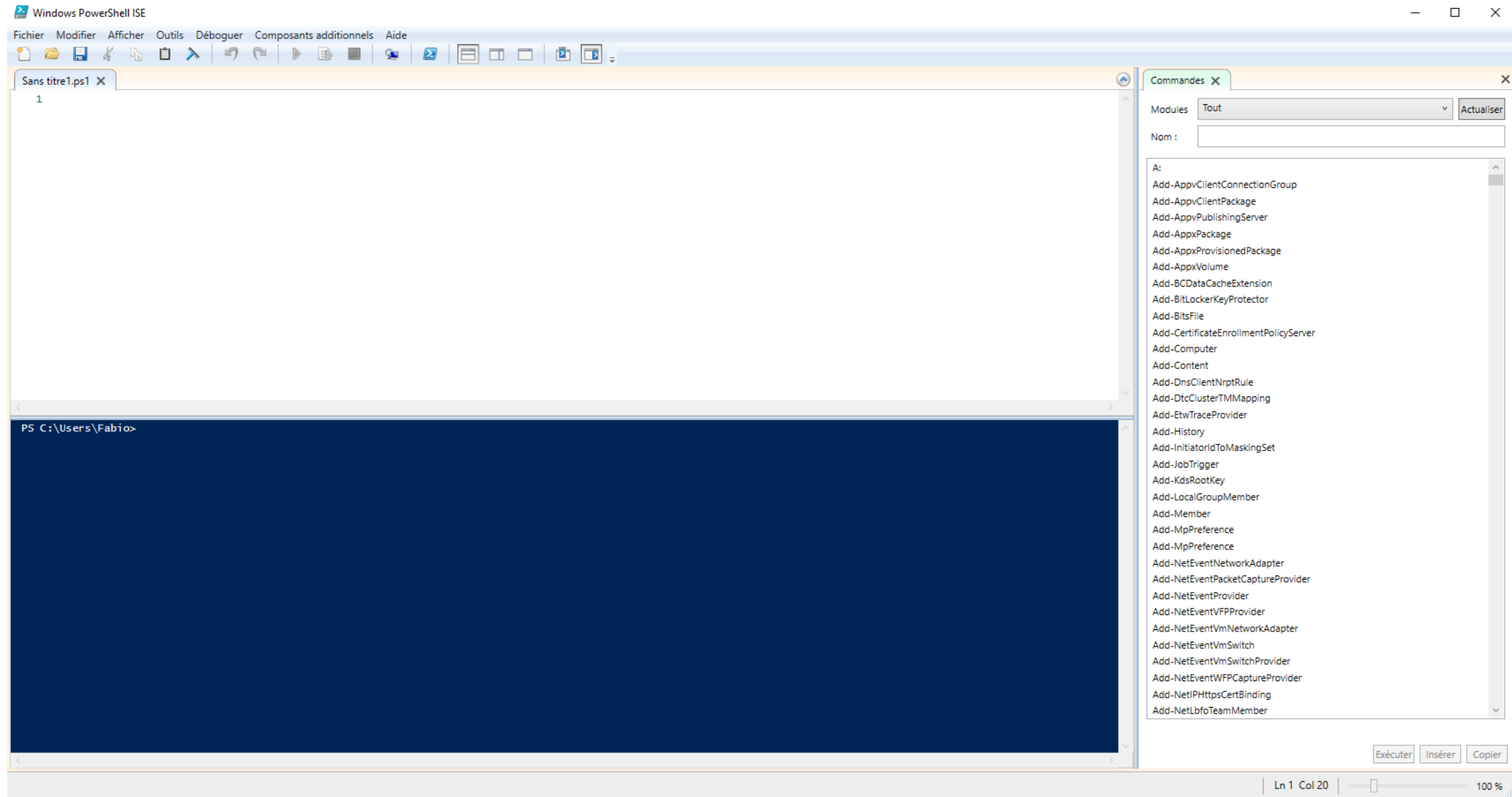
Invite de commandes

```
c:\Windows>dir
Le volume dans le lecteur C s'appelle Local Disk
Le numéro de série du volume est B84C-D958
```

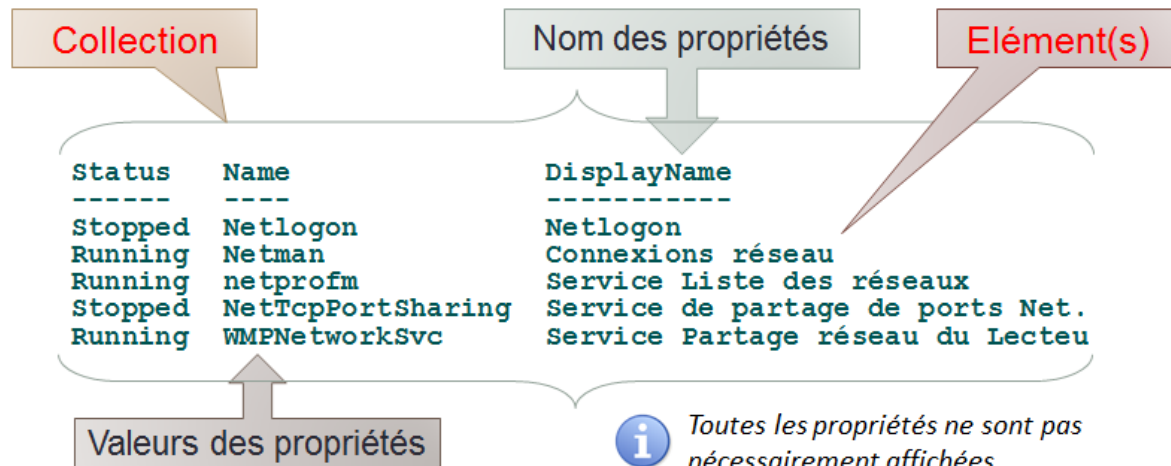
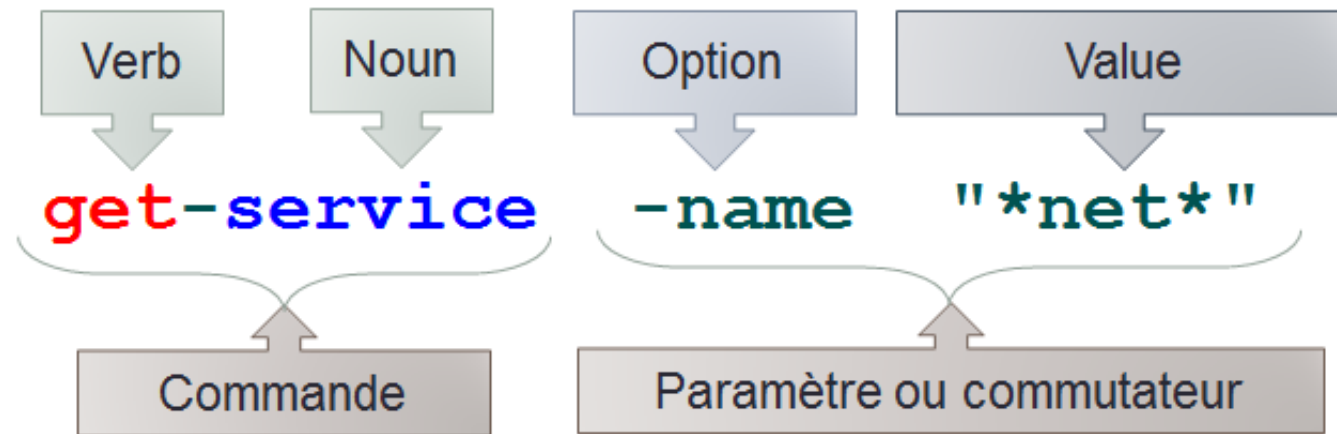
Répertoire de c:\Windows

21/09/2020	15:34	<DIR>	.
21/09/2020	15:34	<DIR>	..
07/12/2019	16:51	<DIR>	addins
26/09/2020	03:22	<DIR>	appcompat
13/10/2020	10:57	<DIR>	apppatch
17/10/2020	18:58	<DIR>	AppReadiness
21/09/2020	15:32	<DIR>	assembly
21/09/2020	16:25	<DIR>	bcastdvr
07/12/2019	11:08		77,824 bfsvc.exe
07/12/2019	11:31	<DIR>	Boot
07/12/2019	11:14	<DIR>	Branding
14/10/2020	11:05	<DIR>	CbsTemp
21/09/2020	15:32		762 comsetup.log
07/12/2019	17:15	<DIR>	Containers
21/09/2020	09:22	<DIR>	CSC
07/12/2019	11:14	<DIR>	Cursors
21/09/2020	15:31	<DIR>	debug
21/09/2020	15:35		7,623 diagerr.xml
07/12/2019	11:31	<DIR>	diagnostics
21/09/2020	16:25	<DIR>	DiagTrack
21/09/2020	15:35		7,623 diagwrn.xml
07/12/2019	16:50	<DIR>	DigitalLocker
07/12/2019	11:17		776 DtcInstall.log

S'entraîner avec l'ISE PowerShell

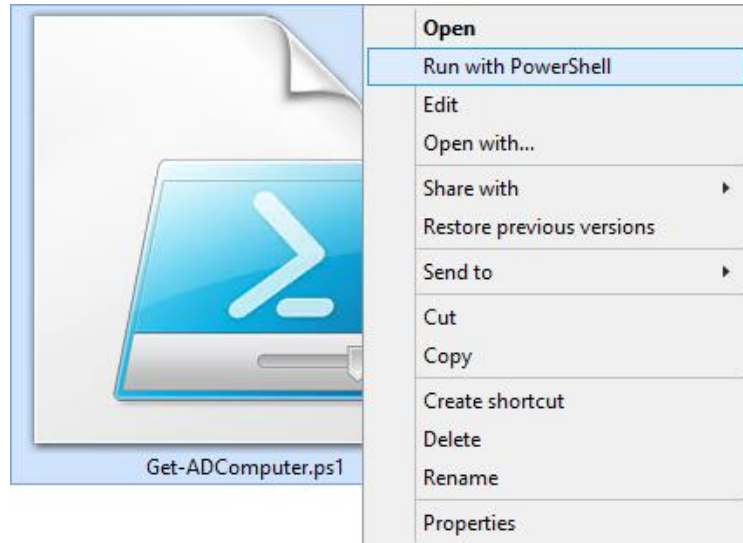


La structure d'une commande



Toutes les propriétés ne sont pas nécessairement affichées

L'exécution des scripts



```
PS C:\Users\Fabio> Get-ExecutionPolicy
Restricted
```

```
PS C:\Users\Fabio>
```

- **Restricted** — Aucun script n'est autorisé. Il s'agit du paramètre par défaut, que vous verrez donc lors de votre première exécution de la commande.
- **AllSigned** — Vous pouvez exécuter les scripts signés par un développeur de confiance. Ce paramétrage vous demandera, avant l'exécution d'un script, de confirmer que vous souhaitez bien l'exécuter.
- **RemoteSigned** — Vous pouvez exécuter vos propres scripts ou les scripts signés par un développeur de confiance.
- **Unrestricted** — Vous pouvez exécuter tous les scripts que vous voulez.

Le format des cmdlets

- **Get** — pour obtenir quelque chose
- **Set** — pour définir quelque chose
- **Start** — pour exécuter quelque chose
- **Stop** — pour arrêter quelque chose en cours d'exécution
- **Out** — pour générer quelque chose
- **New** — pour créer quelque chose (« new » n'est pas un verbe, mais il fonctionne comme un verbe)

Quelques exemples

```
PS C:\Users\Fabio> Get-Process
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
694	116	175872	197036	18,72	148	1	AcroRd32
740	36	19660	48632	2,78	9300	1	AcroRd32
324	20	17680	21284	0,91	3648	0	AnyDesk
285	17	18572	19132	0,48	13752	1	AnyDesk
268	16	4900	18460	0,48	12680	1	ApplicationFrameHost
231	11	2768	3704		4788	0	AppVShNotify
121	8	1572	1156		3704	0	armsvc
515	14	15284	17528	1,48	5680	0	audiodg
138	7	1760	4896	0,11	8760	1	CompPkgSrv
96	7	6216	6076		6156	0	conhost
266	14	4460	16172	0,44	6556	1	conhost
80	7	6300	6106	0,00	18188	1	conhost

```
PS C:\Users\Fabio> Get-Content C:\Windows\System32\drivers\etc\hosts
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com   # source server
#       38.25.63.10       x.acme.com      # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
```

```
PS C:\Users\Fabio> Get-Service
```

Status	Name	DisplayName
Stopped	AarSvc_264bd6	Agent Activation Runtime_264bd6
Running	AcrSch2Svc	Acronis Scheduler2 Service
Running	AdobeARMservice	Adobe Acrobat Update Service
Stopped	AdobeFlashPlaye...	Adobe Flash Player Update Service
Stopped	AJRouter	Service de routeur AllJoyn
Stopped	ALG	Service de la passerelle de la couc...
Running	AnyDesk	AnyDesk Service
Stopped	AppIDSvc	Identité de l'application
Running	Appinfo	Informations d'application
Stopped	AppMgmt	Gestion d'applications
Stopped	AppReadiness	Préparation des applications
Stopped	AppVClient	Microsoft App-V Client

Connaitre les paramètres d'une commande

```
PS C:\Users\Fabio> Get-Process | get-member
```

```
TypeName : System.Diagnostics.Process
```

Name	MemberType	Definition
----	-----	-----
Handles	AliasProperty	Handles = Handlecount
Name	AliasProperty	Name = ProcessName
NPM	AliasProperty	NPM = NonpagedSystemMemorySize64
PM	AliasProperty	PM = PagedMemorySize64
SI	AliasProperty	SI = SessionId
VM	AliasProperty	VM = VirtualMemorySize64
WS	AliasProperty	WS = WorkingSet64
Disposed	Event	System.EventHandler Disposed(System.Object, System.EventArgs)
ErrorDataReceived	Event	System.Diagnostics.DataReceivedEventHandler ErrorDataReceived(System.Object, System.EventArgs)
Exited	Event	System.EventHandler Exited(System.Object, System.EventArgs)
OutputDataReceived	Event	System.Diagnostics.DataReceivedEventHandler OutputDataReceived(System.Object, System.EventArgs)
BeginErrorReadLine	Method	void BeginErrorReadLine()
BeginOutputReadLine	Method	void BeginOutputReadLine()
CancelErrorRead	Method	void CancelErrorRead()



TP 3

TP 3 : La découverte de Powershell

1. Prise en main de Powershell
2. Trouver les commandes pour gérer les fichiers et les dossiers (slide suivante)
3. Récupérer les informations de votre VM d'Hyper-V
 - Etat de la machine
 - RAM...
 - Démarrage de la VM...

Durée maximale : 2h

Dépôt du compte rendu sur Moodle (TP 3)

TP 3 : La découverte de Powershell

- Se déplacer dans les dossiers
- Afficher le chemin du dossier courant
- Afficher le contenu d'un dossier
- Créer un dossier
- Créer un fichier avec du texte
- Supprimer un fichier ou un dossier
- Déplacer un fichier
- Déplacer un dossier
- Renommer un fichier ou dossier
- Copier un fichier
- Copier un dossier avec ses fichiers
- Tester l'existence d'un fichier ou dossier