



CYBER RANGERS  
ARMORING YOUR BUSINESS



# POWERSHELL BASIC SCRIPTING

## MODULE 3: PSDRIVES AND PSPROVIDERS

Jan Marek | Cyber Rangers

OSCP | eCPPT | CEH | CHFI | CompTIA Pentest+ | CEI | MVP | MCT | MCC | MCSA | MCSE

Ethical Hacker, Forensic Investigator & Security Engineer

[jan@cyber-rangers.com](mailto:jan@cyber-rangers.com) | [www.cyber-rangers.com](http://www.cyber-rangers.com)



# AGENDA

- How to enumerate registry, local certificates etc.
- How to work with non-standard data like AD database
- How to map network drives in PowerShell



# PSPROVIDERS

- Data interpreted as hard drives
- Similar approach for data enumeration

Get-PSProvider

Get-PSProvider | Format-Table -Property Name, Capabilities -AutoSize -Wrap



# PSDRIVES

- Represents a connected data store
- Drives use a **PSPProvider** to connect to the store
- Drive names do not include a colon (:)
- Drive paths do include a colon, for example **C:**

## Get-PSDrive

```
New-PSDrive -Name 'windir' -PSPProvider FileSystem -Root 'C:\Windows'
```

```
New-PSDrive -Name 'HKU' -PSPProvider Registry -Root HKEY_USERS
```

```
Set-Location windir:
```

```
Set-Location hku:
```

```
Set-Location env:
```

```
New-PSDrive -Name S -PSPProvider FileSystem -Root \\dc\c$ -Persist
```



# WORKING WITH PSDRIVES: FILESYSTEM, REGISTRY

```
Set-Location C:
```

```
New-Item C:\temp\test1 -ItemType Directory
```

```
Set-Location HKLM:
```

```
Set-Location .\SOFTWARE
```

```
New-Item -Name _Training
```

```
Set-Location .\_Training
```

```
New-ItemProperty -Name Reg1 -Value 1 -Path .
```



# WORKING WITH PSDRIVES: ACTIVE DIRECTORY

```
Get-PSDrive
```

```
Import-Module ActiveDirectory
```

```
Get-PSDrive
```

```
Set-Location AD:
```

```
Get-ChildItem
```

```
Set-Location 'DC=cyber-rangers,DC=lab'
```

```
Get-ChildItem
```

```
Set-Location 'OU=Lab'
```

```
Get-ChildItem | where-object {$_.objectclass -eq 'user'} | select-object -First 1  
-Property *
```

```
Set-Location ..
```

```
New-Item -ItemType user -Path "OU=Lab" -Name "CN=testuser1"
```

```
Set-ItemProperty -Path AD:\"CN=testuser1,OU=Lab,DC=cyber-rangers,DC=lab"
```

```
-Name Company -Value 'Cyber Rangers'
```

# LAB







# POWERSHELL BASIC SCRIPTING

## MODULE 3: PSDRIVES AND PSPROVIDERS

Jan Marek | Cyber Rangers

OSCP | eCPPT | CEH | CHFI | CompTIA Pentest+ | CEI | MVP | MCT | MCC | MCSA | MCSE

Ethical Hacker, Forensic Investigator & Security Engineer

[jan@cyber-rangers.com](mailto:jan@cyber-rangers.com) | [www.cyber-rangers.com](http://www.cyber-rangers.com)



CYBER RANGERS  
ARMORING YOUR BUSINESS