

Wewnątrz maszyny wirtualnej wykonaj poniższe polecenia:

```
Enable-PSRemoting -Force -SkipNetworkProfileCheck
```

```
New-Item -Path 'C:\r2\New Folder' -ItemType Directory
```

```
New-Item -Path 'C:\r2\New Folder\file.txt' -ItemType File -f -v "mmm"
```

```
New-Item -Path 'C:\r2\cars.xml' -ItemType File -f -v "xml_mmm"
```

```
New-Item -Path 'C:\r2\kealtcheck.html' -ItemType File -f -v "html_mmm"
```

```
New-Item -Path 'C:\r2\servicereport.html' -ItemType File -f -v "service_html_mmm"
```

```
New-Item -Path 'C:\r1\New Folder' -ItemType Directory
```

```
New-Item -Path 'C:\r1\New Folder\file.txt' -ItemType File -f -v "mmm"
```

```
New-Item -Path 'C:\r1\cars.xml' -ItemType File -f -v "xml_mmm"
```

```
New-Item -Path 'C:\r1\kealtcheck.html' -ItemType File -f -v "html_mmm"
```

```
New-Item -Path 'C:\r1\servicereport.html' -ItemType File -f -v "service_html_mmm"
```

```
New-Item -Path 'C:\r1\style.css' -ItemType File -f -v "css_mmm"
```

```
New-Item -Path 'C:\r1\test.xlsx' -ItemType File -f -v "xlsx_mmm"
```

```
New-Item -Path 'C:\r1\testcsv.csv' -ItemType File -f -v "csv_mmm"
```

```
New-Item -Path 'C:\r10' -ItemType Directory
```

```
New-Item -Path 'C:\r11' -ItemType Directory
```

```
New-Item -Path 'C:\r12' -ItemType Directory
```

```
New-Item -Path 'C:\d\New Folder' -ItemType Directory
```

```
New-Item -Path 'C:\d\New Folder\file.txt' -ItemType File -f -v "mmm"
```

```
New-Item -Path 'C:\d\cars.xml' -ItemType File -f -v "xml_mmm"
```

```
New-Item -Path 'C:\d\kealtcheck.html' -ItemType File -f -v "html_mmm"
```

```
New-Item -Path 'C:\d\servicereport.html' -ItemType File -f -v "service_html_mmm"
```

```
New-Item -Path 'C:\d\style.css' -ItemType File -f -v "css_mmm"
```

```
New-Item -Path 'C:\d\test.xlsx' -ItemType File -f -v "xlsx_mmm"
```

```
New-Item -Path 'C:\d\testcsv.csv' -ItemType File -f -v "csv_mmm"
```

```
New-Item -Path 'C:\d\Profile' -ItemType Directory
```

```
New-Item -Path 'C:\d\Profile\info.txt' -ItemType File -f -v "info o profilach"
```

```
New-Item -Path 'C:\d\Pliki dyskow' -ItemType Directory
```

```
New-Item -Path 'C:\d\Pliki dyskow\mapuj.txt' -ItemType File -f -v "mapowane dyski"
```

```
New-Item -Path 'C:\d0' -ItemType Directory
```

```
New-Item -Path 'C:\d1' -ItemType Directory
```

```
New-Item -Path 'C:\d1\kealtcheck.html' -ItemType File -f -v "html_mmm"
```

```
New-Item -Path 'C:\d1\test.xlsx' -ItemType File -f -v "xlsx_mmm"
```

```
New-Item -Path 'C:\d1\testcsv.csv' -ItemType File -f -v "csv_mmm"
```

```
New-Item -Path 'C:\d1\cbt.txt' -ItemType File -f -v "cbt_mmm"
```

```
New-Item -Path 'C:\d1\New' -ItemType Directory
```

```
New-Item -Path 'C:\d1\New\file.txt' -ItemType File -f -v "mmm"
```

```
New-Item -Path 'C:\d1\New\about.html' -ItemType File -f -v "about_html"
```

```
New-Item -Path 'C:\d2' -ItemType Directory
```

```
New-LocalUser -Name "7H" -Password (ConvertTo-SecureString "Pa$$w0rd" -AsPlainText -Force)
```

```
Set-LocalUser -Name "7H" -PasswordNeverExpires $true -Description "Opis konta1"
```

```
Add-LocalGroupMember -SID "S-1-5-32-545" -Member 7H
```

```
New-LocalUser -Name "8H" -Password (ConvertTo-SecureString "Pa$$w0rd" -AsPlainText -Force)
```

```
Set-LocalUser -Name "8H" -PasswordNeverExpires $true -Description "Opis konta1"
```

```
Add-LocalGroupMember -SID "S-1-5-32-545" -Member 8H
```

```
uruchom Start-Transcript C:\imienazwisko_33ppk2_grnr.txt
```

```
Utworzenie plik C:\imienazwisko_33rpk2_grnr.txt
```

*** Oznacza twoje inicjały**

Test praktyczny:

1. Wykonaj:

- a. utworzenie bezpiecznego ciągu. Wpisz hasło w interaktywnym wierszu.
Konwertuj z istniejącej zmiennej w postaci zwykłego tekstu.
- b. utworzenie poświadczenia PS. Zakładając, że masz hasło w postaci SecureString w zmiennej \$SecurePassword
- c. wyodrębnienie hasła z PSCredentials
- d. wyodrębnienie hasła z SecureString. Masz tylko SecureString z hasłem, skonstruuj obiekt PSCredentials i Wyodrębnienie hasła przy użyciu poprzedniej metody.
- e. konwertowanie zmiennej SecureString na bezpieczną reprezentację w postaci zwykłego tekstu.

```
$pass = Read-Host "passw: "  
$pass = ConvertTo-SecureString $pass -AsPlainText -Force  
$cred=New-Object -TypeName PSCredential -ArgumentList @('user',$pass)  
$a=[Runtime.InteropServices.Marshal]::SecureStringToBSTR($cred.Password)  
$plain=[Runtime.InteropServices.Marshal]::PtrToStringAuto($a)
```

2. Przedstaw na wycinkach. Za pomocą programu ZIP w systemie Windows 11. Wykonaj:

- a) zabezpieczenie hasłem folderu C:\r2
- b) dodanie plików do zabezpieczonego folderu C:\r2
- c) zastąpienie istniejących plików w folderze C:\r2
- d) odbezpieczenie folderu C:\r2 chronionego hasłem.
winrar

3. Bezpieczne zapisywanie poświadczeń za pomocą PowerShell

- a) Użyj funkcji bezpiecznego ciągu programu PowerShell.
- b) Bezpiecznie zapisz poświadczenia w pliku, aby można było je użyć ponownie później i zachować ochronę.
- c) Zapisz plik sciezka_do_pliku1.xml na komputerze w sieci za pomocą PowerShell i zabezpiecz ten plik za pomocą PowerShell przed nieautoryzowanym dostępem.

Uwaga masz do dyspozycji tylko jeden komputer ładujesz z adresu lub ścieżki sieciowej.

```
$sec = Get-Credential  
$sec | Export-Clixml -Path .\a.xml  
$sec | Export-CliXml -Path \\$env:COMPUTERNAME\c$\1.xml
```

4. Bezpieczne załaduj poświadczenie z pliku z powrotem do zmiennej.

- a) Przeprowadź próbę załadowania poświadczenia z pliku z powrotem do zmiennej ładując plik

Praca praktyczna gr1 v7
z komputera w sieci.

b) Załaduj poświadczenia z pliku z powrotem do zmiennej ładując plik z komputera w sieci

```
$sec1=Import-Clixml -Path \\$env:COMPUTERNAME\c$\1.xml
```

Uwaga masz do dyspozycji tylko jeden komputer ładujesz z adresu lub ścieżki sieciowej.

5. Wdróż szyfrowanie AES za pomocą PowerShell wykonaj

- a) szyfrowanie. Utwórz hasło jako bezpieczny ciąg i zaszyfruj je.
- b) deszyfrowanie. Odszyfruj tekst za pomocą tego samego hasła.

<https://isobczak.zsl.gda.pl/powershell/21%20Szyfrowanie%20danych,%20plik%c3%b3w,%20dysk%c3%b3w/AesEncryption.psm1>

```
$password = Read-Host -AsSecureString  
$enc = Protect-AesString -String 'abc' -Password $password
```

```
$enc | Unprotect-AesString -Password $password
```

6. Za pomocą poleceń PowerShell wykonaj

- a) utworzenie lokalnego konta użytkownika **R*25** nie określaj parametrów konto nie wygasa ani nie ma domyślnie hasła.
- b) utworzenie konta użytkownika **R*35** z złożonym hasłem.
- c) ustawienie daty wygaśnięcia konta użytkownika **R*35** na 12.05.2036.
- d) utworzenie konta użytkownika **R*55** z wskazanym w poleceniu hasłem **Pa\$\$w0rd1**.

```
New-LocalUser -Name "R*25" -AccountNeverExpires -NoPassword  
New-LocalUser -Name "R*35"  
Set-LocalUser -Name "R*35" -AccountExpires $(Get-Date -Year 2036 -Month 05 -Day 12)  
New-LocalUser -Name "R*55" -Password $(ConvertTo-SecureString "Pa$$w0rd1" -AsPlainText -  
Force)
```

”
7. Za pomocą polecenia cmdlet PowerShell

- a) ustaw użytkownika **7H** członkiem grupy Użytkownicy.
- b) dodaj członków **7H** i **8H** do grupy lokalnej **S***.
- c) dodaj użytkownika **R*55** jako członka do grupy Administratorzy.

```
Add-LocalGroupMember -Group 'Użytkownicy' -Member '7H'  
New-LocalGroup -Name 'S*'  
Add-LocalGroupMember -Group 'SKW' -Member '7H'  
Add-LocalGroupMember -Group 'SKW' -Member '8H'  
New-LocalUser -Name 'R*55'  
Add-LocalGroupMember -Group 'Administratorzy' -Member 'R*55'
```

8. Udostępnianie folderu za pomocą PowerShell

- Udostępnij za pomocą PowerShell, folder o nazwie „d” pod nazwą „A*”.
- Przypisz uprawnienia do zmiany i odczytu dla wielu użytkowników, zapewnij dostęp do zmian użytkownikowi 7H i pełny dostęp użytkownikowi 8H do folderu o nazwie „d”.
- Utwórz ukryty folder współdzielony Profile dla grupy Wszyscy, pełny dostęp.
- Pobierz listę ACL udziału Profile, A*.
- Pokaż udziały SMB.

```
New-SmbShare -Path "c:\d" -Name "A*"
Grant-SmbShareAccess -Name "A*" -AccountName "7H" -AccessRight Change
Grant-SmbShareAccess -Name "AKW" -AccountName "8H" -AccessRight Full
New-SmbShare -Name "Profile$" -Path "c:\Profile" -FullAccess Wszyscy
Get-SmbShareAccess "A*"
Get-SMBShare
```

9. Uprawnienia NTFS do plików i folderów w PowerShell

A. Używając cmdletu pobierz reguły dostępu do obiektu C:\d zobacz

- sieciowo: \\STACJA\A*
- szczegółowo jakie uprawnienia są ustawione lokalnie do folderu: C:\d.

B. Wykonaj modyfikowanie uprawnień do folderu.

- Przysznaj użytkownikowi 8H prawo do odczytu folderu C:\d.
- C. Wykonaj kopiowanie uprawnień z C:\d do nowego obiektu C:\B* (Utworzenie go).

```
Get-ACL -Path "C:\d"
Get-ACL -Path \\$env:COMPUTERNAME\A*
Get-ACL -Path "\\$env:COMPUTERNAME\AKW" | fl *
```

```
$ACL = Get-ACL -Path "C:\d"
$acc = New-Object System.Security.AccessControl.FileSystemAccessRule("8H","Read","Allow")
$ACL.SetAccessRule($acc)
$ACL | Set-Acl -Path "C:\d"
Get-Acl -Path "C:\d" | Set-Acl -Path "c:\BKW"
```

Modyfikowanie własności.

- Wykonaj zmianę właściciela C:\d1.
- Uzyskaj więcej informacji na temat C:\d1.

```
$ACL = Get-Acl -Path "C:\d1"
$own = New-Object System.Security.Principal.NTAccount("8H")
$ACL.SetOwner($own)
$acl | Set-Acl -Path "c:\d1"
Get-Acl -Path "C:\d1" | ft -Wrap
```

Zakończenie

Wewnątrz maszyny wirtualnej uruchom **Stop-Transcript**

Po wykonywaniu zadania w folderze Imie_nazwisko_ucznia zapisz pliki wynikowe dokumentujący wykonane zadania.

- A. Wewnątrz maszyny wirtualnej otwórz **C:\imienazwisko_33ppk2_grnr.txt** zaznacz jego zawartość i wybierz kopiuj, na pulpicie maszyny fizycznej w utworzonym folderze Imie_nazwisko_ucznia Utworzenie plik **imienazwisko_33ppk2_grnr.txt** i wybierz wklej. Zamknij pliki.
- B. Wewnątrz maszyny wirtualnej otwórz **C:\imienazwisko_33rp2_grnr.txt** zaznacz jego zawartość i wybierz kopiuj, na pulpicie maszyny fizycznej w utworzonym folderze Imie_nazwisko_ucznia Utworzenie plik **imienazwisko_33rp2_grnr.txt** i wybierz wklej. Zamknij pliki.

Uwaga: Do sprawdzenia oddajemy folder Imie_nazwisko_ucznia na pulpicie maszyny fizycznej w którym znajdują się dwa pliki:

imienazwisko_33ppk2_grnr.txt

imienazwisko_33rp2_grnr.txt