GOPAS

Remote access

Ing. Ondřej Ševeček | GOPAS a.s. |
MCSM:Directory2012 | MCM:Directory2008 | MVP:Enterprise Security | CEH | CHFI | CISA |
ondrej@sevecek.com | www.sevecek.com |

1

Admin accounts to use (all passwords are Pa$$w0rd)

- gps\domain-admin
  - Domain Admins
- gps\db-admin
  - Administrators on DATA server
- gps\iis-admin
  - Administrators on SRV, WFE
- gps\rdp-admin
  - Administrators on RDP
- gps\wks-admin
  - Administrators on WKS

GOPAS

2

User input and passwords

```
$login = Read-Host 'Type your login'
$login.GetType().FullName


# password only [SecureString]
$password = Read-Host 'Type password' -AsSecureString
$password.GetType().FullName

# password only [SecureString]
$securePwd = ConvertTo-SecureString 'Pa$$w0rd' -AsPlainText -Force



# whole credentials [PSCredential]
$credentials = Get-Credential $login -Message 'Login for WMI'
$credentials.GetType().FullName



# plaintext password from the [PSCredential]
$credentials.GetNetworkCredential().Password

# plaintext password from the [SecureString]
(New-Object Management.Automation.PSCredential 'NoLgn', $securePwd
).GetNetworkCredential().Password
```

GOPAS

3

Remote access over SMB (TCP 445)

```
# only SSO aka default credentials
Get-Service -Computer data

# only SSO aka default credentials
Get-Process -Computer data

# runs either under SSO aka default credentials
T:\SysInternals\psexec -noBanner -acceptEula \\wfe
c:\windows\system32\inetsrv\appcmd list apppool /text:*

# or you can also supply credentials in plaintext
# you may have to convert them from [SecureString] or [PSCredential]
$password = 'Pa$$w0rd'
$login = 'gps\domain-admin'
T:\SysInternals\psexec -u $login -p $password -noBanner -acceptEula \\wfe
c:\windows\system32\inetsrv\appcmd list apppool /text:*
```

GOPAS

4

Remote access over the Active Directory Web Services (TCP 9389)

```
$newPassword = ConvertTo-SecureString 'Pa$$w0rdPa$$w0rd' -AsPlain -Force

Get-ADUser stanislav -Credential (Get-Credential gps\domain-admin) |
  Set-ADAccountPassword -Reset -NewPassword $newPassword
```

GOPAS

5

Remote access over Windows Management Instrumentation (WMI) (TCP 135 + TCP DCOM)

```
$cred = Get-Credential gps\domain-admin

Get-WmiObject Win32_LogicalDisk $cred -Computer data

(gwmi -List Win32_Process -Computer wfe -Cred $cred).Create('mspaint')
```

GOPAS

6

Remote access over Windows Remote Management (WinRM) (TCP 5985)

```
$cred = Get-Credential gps\domain-admin
$session = New-CimSession -Credential $cred -Computer data

Get-CimInstance Win32_LogicalDisk -CimSession $session

Invoke-CimMethod -CimSession $session `
                 -Class Win32_Process `
                 -Method Create `
                 -Arguments @{ CommandLine = 'mspaint' }


$session.Close()
```

GOPAS

7

PowerShell Remoting over WinRM (TCP 5985)

```
# you may need to Enable-PSRemoting on workstation operating
systems and Windows 2008 R2 and older
# Enable-PSRemoting -SkipNetworkProfileCheck -Force

$cred = Get-Credential gps\domain-admin

Enter-PSSession -Computer data -Credential $cred

Invoke-Command -Computer data `
               -Credential $cred `
               -ScriptBlock { ipconfig; klist }
```

GOPAS

8