

## **Práctica 19. Empleo de RootKit NTRoot (Revista HackXcrack)**

Empecemos diciendo que esta práctica conlleva sus riesgos, en bastantes ocasiones el sistema se vuelve inestable, incluso aunque se recupere el estado original, es muy probable que la máquina “haga cosas raras”, realiza pruebas en un EQUIPO CUYOS DATOS NO SEAN IMPORTANTES.

Descomprime el ZIP: w2k\_rootkit0.40.zip en una carpeta que llamaremos C:\rk y dispondrás de los dos archivos necesarios, que son:

```
_root.sys_ y deploy.exe
```

Ambos los debes situar en la misma carpeta o directorio donde vayas a ejecutar el rootkit, para iniciar el proceso teclea:

```
C:\rk\deploy.exe
```

Una vez ejecutado puedes parar o iniciar el rootkit simplemente poniendo:

```
Net start _root_ → Inicia el rootkit  
Net stop _root_ → Detiene el rootkit
```

Si tienes el antivirus activo, SALTARÁ, es un programa bien conocido por casi todos los antivirus, así que antes de “colarlo” en el objetivo, asegúrate que el mismo está desactivado, además necesitarás acceso como administrador para poderlo ejecutar, vamos que todo son problemas.

Aunque los rootkits son armas potentes y que dejan “vendido” a cualquier sistema ante nuestros pies, en seguida son detectados (precisamente por ese peligro potencial) y las fabricantes de “Anti-Bichos” se ponen rápidamente manos a la obra, por lo que en breve será detectado por ellos, claro si es que no lo has colado ya...

### **Como Funciona**

El mecanismo es sencillo de comprender, este rootkit OCULTA cualquier cosa (archivo, proceso, servicio, carpeta, etc.) que comience por *\_root\_*, por ejemplo y para seguir con nuestro troyano, sigue estos pasos:

- 1º) nos situamos en el directorio rk, donde se ha descomprimido el rootkit
- 2º) Ejecutamos *deploy.exe*
- 3º) *Netstart \_root\_*
- 4º) Accedemos a la carpeta donde tenemos nuestro troyano C:\winnt\system32,

```
CD C:\winnt\system32
```

- 5º) Creamos una carpeta oculta utilizando el método del rootkit

```
MD _root_NOMEVES
```

- 6º) copiamos los archivos troyanizados y los cambiamos el nombre,

```
COPY mdsn32.exe c:\_root_NOMEVES\_root_su.exe  
COPY usbkeyb.dll c:\_root_NOMEVES\_root_su.ini
```

Los nombres que pongas no importa, lo que si es relevante es que comiencen por *\_root\_*

7º) Borramos los archivos troyanizados de la carpeta winnt\system32

```
DEL mdsn32.exe
DEL usbkeyb.dll
```

El motivo es que ya no los necesitaremos allí, los tenemos OCULTOS por el rootkit

8º) Accedemos a la carpeta raiz

```
DIR C:\
```

Y la carpeta \_root\_NOMEVES, simplemente NO APARECE.  
PERO ESTÁ TE LO ASEGURO

```
CD _root_NOMEVES
DIR
```

LOS ARCHIVOS renombrados NO APARECEN  
Y no aparecerán NUNCA JAMAS, amenos que uses net stop \_root\_

Sin embargo los puedes ejecutar, prueba:

```
su.exe su.ini -h
```

Observa que se ejecutan con sus nombres verdaderos, sin \_root\_ “por delante”

Bien, ¿y qué? Esto ya lo resolvimos antes, no?, vale pues abre el administrador de tareas, pincha en procesos y ...NO ESTÁ, te lo digo de otra forma, no sólo desaparecieron los archivos es que el proceso es como si no existiera, PERO EXISTE.

Claro estás pensando.... pero la carpeta rk, sí está. Bueno fácil solución:

```
CD\
DEL C:\rk\*.*/s
RD rk
```

## Sugerencias

En una carpeta oculta por el rootkit, cuyo nombre sólo conoces tú, por ejemplo \_root\_softagogo Podemos “almacenar” de todo, Warez, Vídeo, MP3, lo que queramos y todo ello SIN QUE SE DE CUENTA NADIE, ni siquiera el Administrador, simplemente NO SE VE, imagina cientos de Megs, Gigas SOLO PARA TI y para “tus amigos”

Si metemos un virus o un troyano con \_root\_troyano.exe NO LO DETECTARÁ NADIE, ni el antivirus...

Y, lo más de lo más....

Si en el registro añades la clave (como hicimos antes) pero precedida por \_root\_adobegama y su valor correspondiente, esto es:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
```

Y su valor

```
_root_jaja REG_SZ C:\_root_NOMEVES\sus.exe C:\_root_NOMEVES\sus.ini -h
```

Nuestro troyano se ejecutará en el próximo reinicio y NO APARECERÁ en el registro. Hacke Mate.

**Compréndelo bien**

No sería preciso ocultar los archivos, basta con esconder la carpeta y/o el valor del registro.

Aunque los procesos no se vean, si la aplicación “rootkiteda” genera avisos, errores, iconos en la bandeja del sistema, pantallas de inicio o lo que sea, éstos SI SE VERÁN, por ello se sigue incluyendo la opción -h, de nuestro serv-U o como se llame ahora.

La diferencia entre esto y las prácticas anteriores es simplemente que, hasta ahora se “engañaba” al usuario disfrazando el nombre del proceso, archivo, etc. Ahora SE OCULTA no hace falta estrujarse la mente buscando nombres poco llamativos, da igual, NO SE VEN, vamos que a quien engañamos es al mismísimo Sistema Operativo.

Advierte que no sólo podemos esconder un servidor FTP, puede ser cualquier cosa, desde otro tipo de servidor, podemos “montarle” un servidor web o un servidor de correo para “usarlo” a nuestra voluntad ¿Qué mejor servidor anónimo que este?, pero también podemos incluir un keylogger, un “registrador” de teclas pulsadas para averiguar contraseñas o lo que escriba el Santo Inocente.

Seguro que se te ocurren muchas más cosas, pues ala!, les pones sal y limón y a triunfar.

Recuerda que además del delito que comete un hacker al utilizar un rootkit contra la máquina intervenida, lo está cometiendo también contra la propiedad intelectual del Software de Microsoft, así que mucho cuidado con lo que haces.

### La defensa

Ya se comentó en su momento, desde la restauración TOTAL del sistema y sus datos, NADA DE BINARIOS, hasta el chequeo y comprobación de los contenidos de carpetas, si se dispone de una copia segura todo será más fácil.

No te olvides de la prevención, para Windows los rootkits son bien conocidos por los antivirus, mantén actualizadas tus defensas y dormirás algo más tranquilo.