

Práctica 18. Manipulando el Registro de Windows. (Por HxC Mods-Adm)

Ya sabemos cómo editar, modificar y/o añadir nuevas claves con regedit, pero eso supone “estar sentado” físicamente en la máquina objetivo o disponer “de control remoto” de la misma y eso todavía no sabemos hacerlo, ¿Se podrá?

Lo que vamos a usar en esta práctica son determinadas utilidades que nos van a facilitar la tarea a la hora de manejar el Registro prescindiendo de Regedit o de Regedt32.

Conociendo la misión:

Se trata de escribir las nuevas claves a añadir o modificar, podemos utilizar el bloc de notas o algún editor ascii, NO USES WORD o cualquier otro tipo de Tratamiento de Textos que incluya “formatos extraños”, lo que necesitamos es que sea texto claro y limpio del tipo bloc de notas o similar.

Una vez escritas las claves a añadir o modificar, “colocarlas” en el Registro como si lo hubiésemos hecho directamente.

Necesitamos y disponemos de



Como eres bastante observador, imagino que empiezas a conocer de qué van.

Regback: Copia el Registro

Regdmp: Muestra/Vuelca el contenido del registro

Regfind Busca valores y/o datos en el registro

Regini: añade, modifica o elimina claves, valores y datos en el registro

Regrest: restaura una copia del registro

Ya tenemos todo, nos falta aprender su uso, sintaxis y experimentar.

Todas estas herramientas en definitiva hacen lo mismo que la interface gráfica de Regedit, pero no necesitaremos regedit....

Bien, por ahora el que nos interesa es regini.exe, vamos a explicar como funciona:

Por un lado hay que tener un archivo de texto con extensión *.ini con los valores a modificar

Por otro lado hay que conocer cómo se interpretan los valores

Por último hay que conocer la sintaxis del programa

Interpretación de regini.exe de las claves principales del registro

HKEY_LOCAL_MACHINE es convertida a **\Registry\Machine.**

HKEY_USERS equivale a **\Registry\User.**

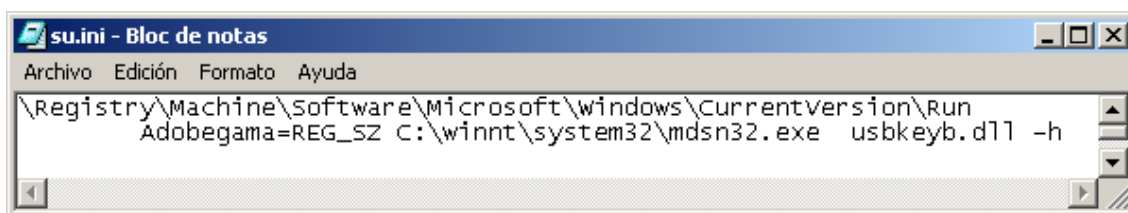
HKEY_CURRENT_USER se convierte en **\Registry\User\User_SID**

Observa todas las entradas comienzan por \Registry, a nosotros nos interesa la primera \Registry\Machine

Lo que queremos es realizar la misma operación que en la práctica anterior, modificar el registro añadiendo los valores necesario tal y como se hizo utilizando regedit.

Foro de HackXcrack

Vamos a crear el archivo .ini, le llamaremos su.ini, abrimos el bloc de notas y escribimos:



Observa la segunda línea es exactamente lo mismo que escribimos cuando se hizo manualmente mediante regedit, en la siguiente tabla se muestran los valores y tipos de dato que aceptan las claves y valores del registro para ser usadas mediante scripts del tipo *.ini

| Tipo de Dato | Valor | Entrada al Registro | Notas |
|------------------|-----------------------------------|---------------------|--|
| REG_SZ | Cadena Caracteres | REG_SZ | REG_SZ tipo de dato por defecto |
| REG_EXPAND_SZ | Cadena Caracteres | REG_EXPAND_SZ | |
| REG_MULTI_SZ | Una o más cadenas entrecomilladas | REG_MULTI_SZ | |
| REG_MULTI_SZFILE | Ruta del fichero | REG_MULTI_SZ | Abre el archivo que indica |
| REG_DWORD | Número decimal | REG_DWORD | 0x para Hexadecimal 0o Octal 0b Binario True, False se convierte a 0x00000001 y 0x00000000 |
| REG_BINARY | Dos o mas números decimales. | REG_BINARY | El primer valor es el número de bytes de los datos que siguen. El resto se convierte en formato de 32 bytes |
| REG_BINARYFILE | Ruta hacia un fichero | REG_BINARY | Se abre el fichero y su contenido se almacena en el registro como valor. La longitud del valor es la longitud del fichero |
| DELETE | Sin valor | Sin valor | Elimina la entrada. |

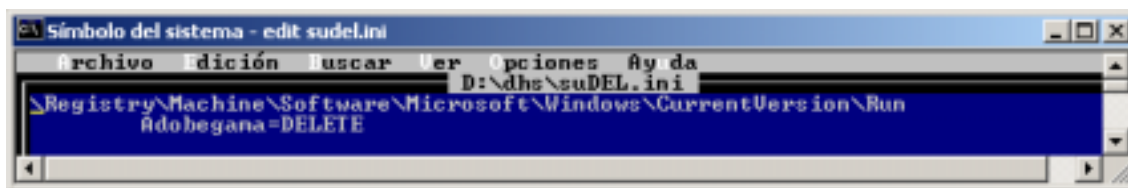
Para añadir el archivo su.ini que acabamos de crear a la entrada correspondiente del registro, hay que escribir:

Regini.exe [dirección_IP] archivo.ini, es decir:

Regini.exe su.ini, para nuestro equipo local o

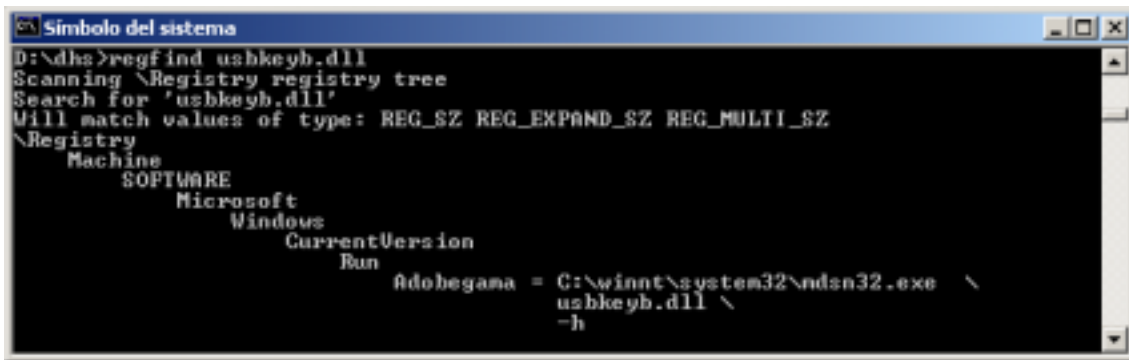
Regini.exe [\\192.168.0.1](#) su.ini, si la ip remota fuese 192.18.0.1

Para eliminar la entrada, crearíamos un archivo.ini, como este:



Lo grabamos, con el nombre sudel.ini y ejecutamos: Regini.exe sudel.ini

Para encontrar una dato o valor, puedes usar regfind.exe, como sigue



```
Símbolo del sistema
D:\dhs>regfind usbkeyb.dll
Scanning \Registry registry tree
Search for 'usbkeyb.dll'
Will match values of type: REG_SZ REG_EXPAND_SZ REG_MULTI_SZ
\Registry
  Machine
    SOFTWARE
      Microsoft
        Windows
          CurrentVersion
            Run
              adobegama = G:\winnt\system32\adsn32.exe \
                usbkeyb.dll \
                -h
```

Sugerencias

Podemos crear un script o fichero *.bat con los pasos para instalar la clave, “subirlo” o guardarlo en la máquina objetivo para que se auto ejecute y “cargue” el troyano, después que se auto elimine. Atrévete.