Interacting with the Registry a11y.text Interacting with the Registry The Windows registry is a magical place where, with just a few keystrokes, you can render a system virtually unusable. So, be very careful on this next section as mistakes can be painful. Meterpreter has some very useful functions for registry interaction. Letâ€™s look at the options.

```
meterpreter > reg
Usage: reg [command] [options]


Interact with the target machine's registry.


OPTIONS:


    -d   The data to store in the registry value.
    -h        Help menu.
    -k   The registry key path (E.g. HKLM\Software\Foo).
    -r   The remote machine name to connect to (with current process credentials
    -t   The registry value type (E.g. REG_SZ).
    -v   The registry value name (E.g. Stuff).
    -w        Set KEY_WOW64 flag, valid values [32|64].
COMMANDS:


    enumkey     Enumerate the supplied registry key [-k ]
    createkey   Create the supplied registry key  [-k ]
    deletekey   Delete the supplied registry key  [-k ]
    queryclass Queries the class of the supplied key [-k ]
    setval      Set a registry value [-k  -v  -d ]
    deleteval   Delete the supplied registry value [-k  -v ]
    queryval    Queries the data contents of a value [-k  -v ]
```

Here we can see there are various

options we can use to interact with the remote system. We have the full options of reading, writing, creating, and deleting remote registry entries. These can be used for any number of actions, including remote information gathering. Using the registry, one can find what files have been used, web sites visited in Internet Explorer, programs used, USB devices used, and so on. There is a great quick reference list of these interesting registry entries published by Access Data, as well as any number of Internet references worth finding when there is something specific you are looking for. Next Persistent Netcat Backdoor Prev Fun with Incognito