Reg Command

Adding Keys and Values:

```
C:\> reg add
[\\TargetIPaddr\][RegDomain]\[Key]
```

Add a key to the registry on machine **[TargetIPaddr]** within the registry domain **[RegDomain]** to location **[Key]**. If no remote machine is specified, the current machine is assumed.

Export and Import:

```
C:\> reg export [RegDomain]\[Key]
[FileName]
```

Export all subkeys and values located in the domain **[RegDomain]** under the location **[Key]** to the file **[FileName]**

```
C:\> reg import [FileName]
```

Import all registry entries from the file **[FileName]**

Import and export can only be done from or to the local machine.

Query for a specific Value of a Key:

```
C:\> reg query
[\\TargetIPaddr\][RegDomain]\[Key] /v
[ValueName]
```

Query a key on machine **[TargetIPaddr]** within the registry domain **[RegDomain]** in location **[Key]** and get the specific value **[ValueName]** under that key. Add /s to recurse all values.

WMIC

Fundamental grammar:

```
C:\> wmic [alias] [where clause] [verb
clause]
```

Useful **[aliases]**:

process **service**
share **nicconfig**
startup **useraccount**
qfe (Quick Fix Engineering – shows patches)

Example **[where clauses]**:

```
where name="nc.exe"
where (commandline like "%stuff")
where (name="cmd.exe" and
    parentprocessid!="[pid]")
```

Example **[verb clauses]**:

```
list [full|brief]
get [attrib1,attrib2…]
call [method]
delete
```

List all attributes of **[alias]**:

```
C:\> wmic [alias] get /?
```

List all callable methods of **[alias]**:

```
C:\> wmic [alias] call /?
```

Example:

List all attributes of all running processes:

```
C:\> wmic process list full
```

Make WMIC effect remote **[TargetIPaddr]**:

```
C:\> wmic /node:[TargetIPaddr]
/user:[User] /password:[Passwd] process
list full
```

Windows Command Line Cheat Sheet

By Ed Skoudis

POCKET REFERENCE GUIDE

SANS INSTITUTE
http://www.sans.org

Purpose

The purpose of this cheat sheet is to provide tips on how to use various Windows command that are frequently referenced in SANS 504, 517, 531, and 560.

Process and Service Information

List all processes currently running:

```
C:\> tasklist
```

List all processes currently running and the DLLs each has loaded:

```
C:\> tasklist /m
```

Lists all processes currently running which have the specified **[dll]** loaded:

```
C:\> tasklist /m [dll]
```

List all processes currently running and the services hosted in those processes:

```
C:\> tasklist /svc
```

Query brief status of all services:

```
C:\> sc query
```

Query the configuration of a specific service:

```
C:\> sc qc [ServiceName]
```

Shutdown and Restart

Shutdown Windows immediately:
`C:\> shutdown /s /t 0`

Note: Command may not power down the hardware.

Restart Windows immediately:
`C:\> shutdown /r /t 0`

Abort shutdown/restart countdown:
`C:\> shutdown /a`

Useful Netstat Syntax

Show all TCP and UDP port usage and process ID:
`C:\> netstat –nao`

Look for usage of port `[port]` every `[N]` seconds:
`C:\> netstat –nao [N] | find [port]`

Dump detailed protocol statistics:
`C:\> netstat –s –p [tcp|udp|ip|icmp]`

Installing Built-in Packages on Vista

Install telnet service on Vista:
`C:\> pkgmgr /iu:"TelnetServer"`

Install telnet client on Vista:
`C:\> pkgmgr /iu:"TelnetClient"`

Install IIS on Vista:
`C:\> pkgmgr /iu:IIS-WebServerRole;WAS-WindowsActivationService;WAS-ProcessModel; WAS-NetFxEnvironment;WAS-ConfigurationAPI`
To remove any of these packages, replace install update (/iu) with uninstall update (/uu)

File Search and Counting Lines

Search directory structure for a file in a specific directory:
`C:\> dir /b /s [Directory]\[FileName]`

Count the number of lines on StandardOuy of `[Command]`:
`C:\> [Command] | find /c /v ""`

Finds the count (/c) of lines that do not contain (/v) nothing (""). Lines that do not have nothing are all lines, even blank lines, which contain CR/LF

Command Line FOR Loops

Counting Loop:
`C:\> for /L %i in ([start],[step],[stop]) do [command]`

Set `%i` to an initial value of `[start]` and increment it by `[step]` at every iteration until its value is equal to `[stop]`. For each iteration, run `[command]`. The iterator variable `%i` can be used anywhere in the command to represent its current value.

Iterate over file contents:
`C:\> for /F %i in ([file-set]) do [command]`

Iterate through the contents of the file on a line-by-line basis. For each iteration, store the contents of the line into `%i` and run `[command]`.

Invoking Useful GUIs at the Command Line

Local User Manager (includes group management):
`C:\> lusrmgr.msc`

Services Control Panel:
`C:\> services.msc`

Task Manager:
`C:\> taskmgr.exe`

Security Policy Manager:
`C:\> secpol.msc`

Event Viewer:
`C:\> eventvwr.msc`

Control Panel:
`C:\> control`

Close GUI windows by hitting Alt-F4

Interacting with the Network Using Netsh

Turn off built-in Windows firewall:
`C:\> netsh firewall set opmode disable`

Configure interface "Local Area Connection" with `[IPaddr] [Netmask] [DefaultGW]`:
`C:\> netsh interface ip set address local static [IPaddr] [Netmask] [DefaultGW] 1`

Configure DNS server for "Local Area Connection":
`C:\> netsh interface ip set dns local static [IPaddr]`

Configure interface to use DHCP:
`C:\> netsh interface ip set address local dhcp`