Useful Analyst Commands

OS	Command	Details
	`systeminfo`	General OS Info
	`schtasks`	Scheduled Tasks

	`net`
	
	`[ accounts | computer | config | continue | file | group | help | localgroup | pause | session | share | start | statistics | stop | time | use | user | view ]`
		Used to connect to, remove, and configure connections to shared resources, like mapped drives and network printers.

	`ipconfig`	Displays all current TCP/IP network configuration values and refreshes ipconfig displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.
	`ifconfig`	
	`tasklist`	Display a list of currently running tasks
	`ps`	
	`top`	
	`netstat -aon`	Display all active connections
	`openfiles`	Enables an administrator to query, display, or disconnect files and directories that have been opened on a system.
	`driverquery`	Enables an administrator to display a list of installed device drivers and their properties.
	`wmic`	Command-line interface for Windows Management Instrumentation (WMI)
	`nslookup`	DNS lookup utility, finding the IP address of a domain name.
	`host`	
	`ddrescue`	A data recovery tool. Copies data from one file or block device (hard disc, cdrom, etc) to another, trying to rescue the good parts first in case of read errors.
	`fltmc`	View drivers filter stack
	`awk`	Domain-specific language designed for text processing and typically used as a data extraction and reporting tool.