Tool Reference: Windows Command Line

General Commands

cd – This command allows you to navigate the filesystem by entering a specified directory

cd .. - This command allows you to navigate the filesystem by taking a step back to the parent of the current directory

dir – This command will display the contents of a directory

echo - This command will display the username of the user running this command

type - This command will display the contents of a file

move - This command will move a specified file to a specified location

copy - This command will copy a specified file to a specified location

del - This command will remove the specified file

findstr -This command allows the user to search though the whole file system to file a specified file

reg query – This command allows you to query registry keys

[command] /? - This command will display information about the specified command and its switches)

systeminfo - This command outputs system information

wmic qfe list – This command will display the patch level of the OS

netsh firewall show state – This command will display the status of the windows firewall

wmic startup list full – This command will display all the process that begin on startup

driverquery – This command will display all installed drivers

vssadmin list shadows – This command will display all shadow copies

Review OS and Application Logs

All OS and Application logs can be Reviewed in the Event Viewer Application

Review User Accounts

net user – This command will display the username of the user running this command

net localgroup administrators – This command will display all users in the Local Administrators group

query user - This command will display the username of all logged in users

net group "Domain Admins" This command will display all users in the Domain Administrators group

wmic useraccount – This command allows you to interect and manage user accounts

Review Running Processes

tasklist – This command will display a list of running processes

Get-Processes – This is a Powershell Commandlet (Cmdlets) that preform a task like **tasklist**

Review Running Services

net start – This command will display a list of running services

tasklist /svc - This command will list services running under each process

Get-Service - This is a Powershell Commandlet (Cmdlets) that preform a task like **net start**

Review Scheduled Tasks

schtasks – This command allows you to interact with all Scheduled Tasks

Get-ScheduledTask - This is a Powershell Commandlet (Cmdlets) that preform a task like **schtasks**

Review Networking Infomation

ipconfig /all - This command shows IP information for the system

route print - This command displays the system's routing table

netstat - This command allows you to interact with networking information on the system