**Windows Commands**

**Incident Response**

|  |  |
| --- | --- |
| tasklist /s [SERVER] | List running processes remotely |
| taskkill /s [SERVER] /PID [PID] | Kill the specified process remotely |
| Remove-ItemProperty -Path "HKLM:\Software\SmpApplication" -Name "SmpProperty" | Remove the SmpProperty registry value from the SmpApplication subkey |

**Sysmon**

|  |  |
| --- | --- |
| sysmon -accepteula -i config.xml | Install Sysmon with the specified configuration file |
| sysmon -c new\_config.xml | Reconfigure Sysmon with a new config file |

**Event Logs**

|  |  |
| --- | --- |
| Get-WinEvent -Path [FILE PATH]/sysmon.evtx | Load logs from the specified .evtx file |
| Get-WinEvent -LogName Microsoft-Windows-Sysmon/Operational -ComputerName [HOST] -Credential | Retrieve Sysmon logs from remote server |
| Import-Clixml -Path [PATH]/events.xml | Import powershell .xml object |
| Import-Clixml -Path [PATH] | Sort TimeCreated | Unique -AsString | Filters out duplicate events; this is due to the non-specific “TimeCreated” time stamp |
| $Events | ft processid,user,commandline | Format-table view and specify columns |