|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Source | Event ID | EventType or EventDescription | EventField | Details |
| Sysmon | 1 | Process Create | ParentCommandLine | C:\Windows\System32\wbem\wmiprvse.exe -secured -Embbeding |
| Sysmon | 1 | Process Create | ParentImage | C:\Windows\System32\wbem\wmiprvse.exe |
| Windows | 4624 | Remote Logon | SourceNetworkAddress | NOT Local IP |
|  |  |  |  |  |

Execution

Lateral Movement

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Source | Event ID | EventType or EventDescription | EventField | Details |
| Sysmon | 1 | Process Create | ParentImage | svchost.exe |
| Sysmon | 1 | Process Create | Image | wsmprovhost.exe |