IRWPX Challenge

Narrative:

OFPOR TTPs

|  |
| --- |

BLUFOR TTPs

|  |
| --- |

Word Picture

|  |
| --- |

RFIs

|  |
| --- |

IRWPX Solution

Artefact: https://github.com/Yamato-Security/hayabusa-sample-evtx/blob/main/EVTX-to-MITRE-Attack/EVTX\_full\_APT\_attack\_steps/ID4688%2C5140%2C5145-WMIexec%20execution%20via%20SMB%20(GLOBAL).evtx

OFPOR TTPs

| **Execution,T1047:**  Windows Management Instrumentation,Remote command via WMI.  **Execution,T1059.003:**  Command and Scripting Interpreter: Windows Command Shell,Cmd.exe quiet execution.  **Lateral Movement,T1021.002:** Remote Services: SMB/Windows Admin Shares,ADMIN$ share access.  **Credential Access / Lateral Movement,T1078.003:** Valid Accounts: Local Accounts,Admin creds NTLM logon.  **Defense Evasion,T1070.001:** Indicator Removal: Clear Windows Event Logs,Audit log cleared.  **Privilege Escalation / Defense Evasion,T1134.001:**  Access Token Manipulation: Token Impersonation/Theft,Token impersonation used.  **Discovery,T1012:**  Query Registry,Registry keys queried.  **Privilege Escalation,T1068:**  Exploitation for Privilege Escalation,Privileges assigned/abused. |
| --- |

BLUFOR TTPs

| **Process Spawn Analysis (D3-PSA)** Analyzes process creation to detect anomalous WMI invocations.  **Decoy File (D3-DF)** Deceives by spoofing executable scripts.  **Client-server Payload Profiling (D3-CSPP)**Analyzes intranet network traffic for anomalous SMB patterns.  **[Account Locking (D3-AL)**,**User Account Permissions (D3-UAP),Domain Account Monitoring (D3-DAM) ]** Disables or restricts user accounts; monitors domain accounts.  **Event Log Analysis (D3-ELA)** Detects modifications to event logs.  **Restore Configuration (D3-RC)** Restores modified firewall configurations.  **Authentication Cache Invalidation (D3-ACI)** Deletes or invalidates access tokens.  **Application Hardening (D3-AH)** Prevents exploitation via code segment modifications. |
| --- |

Word Picture

| An adversary connected to the network on IP 10.23.123.11, likely using Impacket's wmiexec.py, authenticated remotely via NTLM V2 as the admin account "admmig". They accessed the ADMIN$ share over SMB to stage temporary output files and executed quiet commands through WMI, spawning cmd.exe for operations like directory changes with redirected output (typical of wmiexec.py). |
| --- |

RFIs

|  |
| --- |