IRWPX Challenge

Narrative: The local network defenders flagged some suspicious commands being executed on a workstation. Investigate the workstations event logs to confirm suspicious activity.

OFPOR TTPs

|  |
| --- |

BLUFOR TTPs

|  |
| --- |

Word Picture

|  |
| --- |

RFIs

|  |
| --- |

IRWPX Solution

OFPOR TTPs

| **Initial Access (TA0001),T1078: Valid Accounts** admmig network logon via NTLM  **Initial Access (TA0001) / Execution (TA0002),T1210:** **Exploitation of Remote Service**  MS17-010 exploitation for RCE over SMB (file access)  **Execution (TA0002),T1059.003:Command and Scripting Interpreter** cmd.exe launches hidden PowerShell (Event 4688)  **Execution (TA0002),T1059.001:** **Command and Scripting Interpreter:** PowerShell,PowerShell with base64/gzip obfuscation (Event 4688)  **Execution (TA0002) / Defense Evasion (TA0005),T1055**: Process Injection Payload injects shellcode via VirtualAlloc/CreateThread  **Defense Evasion (TA0005),T1027:** **Obfuscated Files or Information** Base64/gzip encoded payloads in PowerShell  **Discovery (TA0007),T1083:** **File and Directory Discovery** Directory enumeration via shares (Events 5140/5145)  **Lateral Movement (TA0008),T1021.002:** **Remote Services: SMB/Windows Admin Shares** ADMIN$/C$/IPC$ share accesses (Events 5140/5145)  **Command and Control (TA0011),T1219: Remote Access Software** IPC$/srvsvc pipes for RPC (Events 5140/5145) |
| --- |

BLUFOR TTPs

| Software Update (D3-SU)  Network Isolation (D3-NI), Inbound Traffic Filtering (D3-ITF)  User Account Permissions (D3-UAP), Credential Hardening (D3-CH)  Network Flow Analysis (D3-NFA), Protocol Metadata Anomaly Detection (D3-PMAD)  Process Spawn Analysis (D3-PSA), Service Process Analysis (D3-SPA) Execution Prevention (D3-EP) Script Execution Analysis (D3-SEA) Process Segment Execution Prevention (D3-PSEP) |
| --- |

Word Picture

| An adversary connected to the network on IPs 10.23.23.9 and 10.23.123.11, likely using Metasploit's ms17\_010\_psexec module, authenticated remotely via NTLM V2 and Kerberos as the admin account "admmig". They accessed the ADMIN$, C$, and IPC$ shares over SMB to stage exploit artifacts like "MS17\_010\_psexec.evtx" and executed remote services through named pipes , spawning cmd.exe to launch obfuscated PowerShell commands with base64-encoded and gzip-compressed payloads. Based on the Windows API’s called in the encoded payload it is likely shell code to be run in the memory of a process. |
| --- |