Step 6 – Adversary Emulation Complete Documentation

Executive Summary
Successfully completed MITRE Caldera adversary emulation exercise simulating Discovery-phase reconnaissance techniques against Windows 10 endpoint with comprehensive SIEM detection through Wazuh monitoring.

1. Environment Configuration
Systems Involved
• Attack Platform: Kali Linux (192.168.1.79) - MITRE Caldera Server
• Target System: Windows 10 (DESKTOP-IROTPGQ, 192.168.1.80) - Sandcat Agent
• Detection System: Wazuh Manager (192.168.1.78) - SIEM Monitoring

Detection Enhancements Implemented
• Enabled Windows Event ID 4688 (Process Creation with Command Line)
• Deployed Sysmon 15.15 with SwiftOnSecurity configuration
• Configured Wazuh agent to collect Security, Sysmon, and PowerShell logs

2. Adversary Emulation Execution
Operation Details
• Operation Name: T1566_Final_Detection_Test
• Adversary Profile: Discovery
• Execution Mode: Autonomous
• Agent: Sandcat (fbmefm)
• Execution Window: 06:38:04 - 06:43:20 UTC (September 29, 2025)
• Success Rate: 87.5% (7 of 8 techniques completed)

Time (UTC)	MITRE ID	Technique Name	Command	PID	Status
06:38:04	T1033	System Owner/User Discovery	$env:username	6660	Success
06:38:15	T1087.001	Local Account Discovery	Get-WmiObject -Class Win32_UserAccount	292	Success
06:39:10	T1057	Process Discovery	gwmi win32_process with owner filtering	220	Success
06:40:10	T1135	Network Share Discovery	Get-SmbShare | ConvertTo-Json	7108	Success
06:41:00	T1482	Domain Trust Discovery	nltest /dsgetdc:$env:USERDOMAIN	4468	Failed
06:42:00	T1518.001	Security Software Discovery	wmic /NAMESPACE:\\root\SecurityCenter2 PATH AntiVirusProduct GET /value	6632	Success
06:42:30	T1069	Permission Groups Discovery	gpresult /R	8820	Success
06:43:20	T1518.001	Security Software Discovery	Get-WmiObject SecurityCenter AntiVirusProduct	5228	Success

3. Detection Analysis
Wazuh Detection Summary
Detection Rate: 100% (All 8 techniques detected, including the failed attempt)

Event ID 4688 Detections
• nltest.exe - Full command line: /dsgetdc:DESKTOP-IROTPGQ
• gpresult.exe - Full command line: /R
• wmic.exe - Full command line with namespace and query
• whoami.exe - User enumeration
• PowerShell executions - All with parent process sandcat.exe

Sysmon Event ID 1 Detections
• WMIC.exe process creation with:
- Complete command line
- Parent process: PowerShell launched by Sandcat
- File hashes: MD5, SHA256, IMPHASH
- User context: test_admin with High integrity level

Detection Table

MITRE Technique	Ability Name	Caldera Status	Wazuh Detection	Event Types	Command Line Captured
T1033	Identify active user	Success	Detected	4688	$env:username via PowerShell
T1087.001	Identify local users	Success	Detected	4688	Get-WmiObject Win32_UserAccount
T1057	Find user processes	Success	Detected	4688	gwmi win32_process with filtering
T1135	View admin shares	Success	Detected	4688	Get-SmbShare
T1482	Discover domain controller	Failed	Detected	4688	nltest /dsgetdc (attempt captured)
T1518.001	Discover antivirus	Success	Detected	4688, Sysmon 1	wmic AntiVirusProduct GET
T1069	Permission Groups	Success	Detected	4688	gpresult /R
T1518.001	Identify Firewalls	Success	Detected	4688	WMI SecurityCenter query

4. Key Findings
Strengths
1. Complete Process Visibility: Event ID 4688 captured all command executions with full command-line parameters
2. Parent Process Tracking: Identified Sandcat agent as attack vector for all malicious activities
3. Enhanced Telemetry: Sysmon provided file hashes and additional process metadata
4. Real-time Detection: All techniques detected within seconds of execution

Limitations Identified
1. Domain Environment: T1482 (Domain Controller Discovery) failed due to standalone workstation configuration
2. Initial Configuration Gap: Required manual enablement of process auditing and Sysmon deployment
3. Log Volume: Generated significant event data requiring filtering for analysis

5. 100-Word Emulation Report
MITRE Caldera T1566 Adversary Emulation Report - September 29, 2025
Successfully executed comprehensive Discovery-phase adversary emulation against Windows endpoint DESKTOP-IROTPGQ using MITRE Caldera framework. Eight reconnaissance techniques deployed between 06:38-06:43 UTC with 87.5% execution success rate.
EXECUTION RESULTS: Enumerated users (T1033, T1087), processes (T1057), network shares (T1135), security software (T1518), and group policies (T1069) via PowerShell and WMI interfaces. Domain controller discovery failed due to non-domain environment.
DETECTION ANALYSIS: Wazuh achieved 100% detection rate through Event ID 4688 (process creation) and Sysmon Event ID 1 monitoring. Full command-line visibility captured all reconnaissance activities with parent process tracking confirming Sandcat agent as attack vector.
RECOMMENDATION: Current detection posture demonstrates effective coverage against Discovery-phase tactics through comprehensive process monitoring and command-line auditing.

6. Recommendations
Immediate Actions
1. Enable PowerShell Script Block Logging (Event ID 4104) for enhanced visibility
2. Configure alerting rules for reconnaissance tool execution (wmic, nltest, gpresult)
3. Implement behavioral analytics for rapid successive reconnaissance activities

Long-term Improvements
1. Deploy Endpoint Detection and Response (EDR) solution for automated response
2. Establish baseline for normal administrative tool usage
3. Implement network segmentation to limit lateral movement post-reconnaissance
4. Develop detection signatures for Caldera-specific patterns

Assessment Conclusion: Adversary emulation successfully demonstrated reconnaissance capabilities and validated SIEM detection effectiveness. Enhanced logging configuration achieved complete visibility into Discovery-phase attack techniques.