SOC Incident Report - Active Attack Simulation & Forensic Investigation

Incident Summary

A controlled active attack simulation was conducted within a VMware lab environment.
The scenario involved payload generation on Kali Linux, HTTP delivery, execution on Windows (VM),
reverse shell establishment, and post-exploitation activity. The incident was investigated
using Windows Event Logs, Registry artifacts, Wireshark, Splunk, and Wazuh.

Environment

Attacker: Kali Linux VM (192.168.164.xxx)
Victim: Windows 10 x64 (VM) (192.168.164.xxx)
Network: VMware Host-Only Network
SIEM Tools: Splunk, Wazuh
Network Analysis: Wireshark

Attack Timeline

1. Payload generated using msfvenom (reverse_tcp, port 4444).
2. Payload hosted via Python HTTP server.
3. Victim downloaded and executed backup_agent.exe.
4. Reverse TCP connection established to attacker (masked internal IP).
5. Meterpreter session successfully opened.
6. File creation and simulated data exfiltration performed.

Evidence Collected

Event ID 5156 – Outbound connection permitted from Windows (VM) to masked internal IP on port 4444.
Event ID 1001 – Application crash (APPCRASH) confirming execution.
UserAssist Registry Key – Confirms GUI execution via Explorer.
Wireshark Capture – TCP stream observed on port 4444 (~2MB transfer).
Splunk Correlation – Process ID mapped to outbound C2 communication.

MITRE ATT&CK; Techniques Observed

T1204 – User Execution
T1059 – Command Execution
T1071 – Application Layer Protocol (Command & Control)
T1105 – Ingress Tool Transfer
T1041 – Exfiltration Over Command & Control Channel

Impact Assessment

Unauthorized outbound connection established from Windows (VM).
Remote command execution achieved.
File system modifications observed.
Sensitive file accessed (hosts file simulation).
Command and control channel successfully established.

Recommendations

Restrict outbound traffic policies at host and network level.
Monitor Event ID 5156 and process creation logs (4688).
Deploy endpoint detection and response (EDR) solutions.
Restrict execution from Downloads directory.
Implement application whitelisting policies.
Enhance SIEM correlation rules for unusual outbound connections.