MITRE ATT&CK Mapping & Detection Validation

Executive Summary

This project simulates an adversary's attack lifecycle and maps the observed behavior to the MITRE ATT&CK framework. Each technique used during the simulation is documented, and detection logic is developed and tested using Splunk and Windows Sysmon logs. The goal is to demonstrate detection engineering, threat mapping, and validation of real-time monitoring capabilities.

Environment Setup

- Attacker Machine: Kali Linux with Nmap, Netcat, and Python tools
- Victim Machine: Windows 10 with Sysmon installed
- SIEM: Splunk Enterprise receiving Sysmon logs
- Scenario: Simulated internal attack involving lateral movement, script execution, and tool downloads

Mapped Techniques (MITRE ATT&CK)

- T1046 - Network Service Scanning
- T1059 - Command and Scripting Interpreter
- T1105 - Ingress Tool Transfer
- T1021.001 - Remote Services: SSH
- T1082 - System Information Discovery

Detection Logic Examples

- T1046 - Detected via spike in outbound traffic on multiple ports (Nmap scan)
  Splunk Query: index=sysmon EventCode=3 dest_port=* | stats count by dest_port

- T1059 - PowerShell execution with suspicious arguments
  Splunk Query: index=sysmon Image="*powershell.exe" CommandLine="*"

- T1105 - File download with uncommon User-Agent
  Splunk Query: index=web_logs method=GET user_agent!="Mozilla*"

Validation & Findings

- Successfully detected lateral movement and file download events

MITRE ATT&CK Mapping & Detection Validation

- PowerShell commands were logged by Sysmon and visible in Splunk
- One missed technique: no alert for compressed file transfer (needs tuning)
- Confirmed detection coverage for 4/5 ATT&CK techniques

Recommendations

- Enhance alerting for suspicious file types and uncommon user agents
- Use MITRE ATT&CK Navigator to continually map and prioritize detection coverage
- Improve endpoint telemetry with more granular logging (e.g., DNS queries, registry changes)