

Proactive Defense of Active Directory: Adversary Emulation and Detection Engineering using MITRE ATT&CK

Zannatul Mawya Priya

Research Context & Background

- Identity as the New Perimeter
- The Vulnerability of Legacy Protocols.
- Current Development (Adversary Emulation).
- Strategic Shift.

Research Problem

The Validation Gap: A persistent gap exists between assumed defensive capabilities (EDR, SIEM) and actual detection efficacy against chained, multi-stage AD attacks.

Logging Deficiencies: Highly critical techniques like DCSync or Kerberoasting often evade default SIEM auditing completely, appearing as legitimate traffic

Simulated Attack Chain (MITRE ATT&CK)



Research Aim & Objectives

Aim: To design, execute, and evaluate a structured adversary emulation plan targeting AD via MITRE ATT&CK, aiming to identify detection gaps and engineer high-fidelity SIEM alerting rules.

Key Objectives:

- Map AD attack vectors to MITRE ATT&CK.
- Engineer an isolated, virtualized AD forest.
- Simulate APT-style chained attacks.
- Author vendor-agnostic Sigma rules to detect anomalies with low false positives.

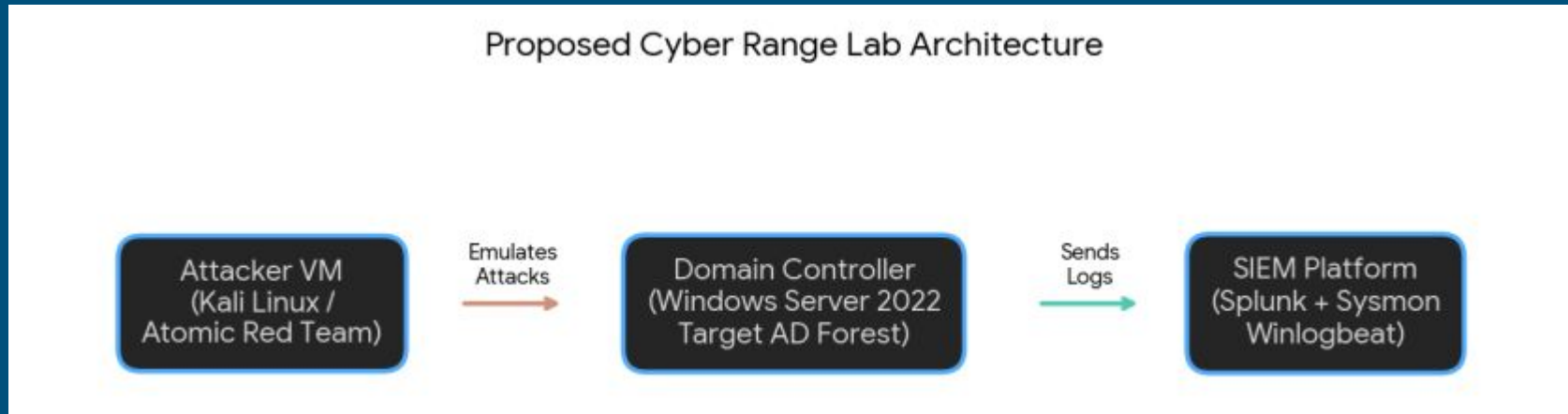
Literature Review & Identified Gap

AD Vulnerabilities: Wright & Smith (2023) document cryptographic mechanics of Kerberoasting flaws.

- Strom et al. (2018) highlight the superiority of MITRE ATT&CK and Purple Teaming over traditional pen-testing.
- While individual AD attacks and theoretical frameworks are well-documented.

Research Methodology & Architecture

Approach: Design Science Research (DSR) & Quantitative Simulation



Red Phase: Execute automated MITRE-mapped payloads via Atomic Red Team.

Blue Phase: Capture Event Logs and Sysmon data to the SIEM.

Purple Phase: Author/test Sigma rules to close visibility gaps.

Data Collection & Evaluation Process

Data Generation: All network and endpoint telemetry (PCAP, Event IDs) will be synthetically and internally generated within the air-gapped Cyber Range [12].

Evaluation Metrics:

Visibility: Did the default logging policy capture the event?

True Positive Rate (TPR): Does the custom Sigma rule successfully trigger an alert upon emulation execution?

False Positive Rate (FPR): Does the rule stay quiet during normal, baseline AD operations?

Project Planning Timeline



Resources: High-performance Hypervisor, Windows Server 2022 ISOs, Splunk Enterprise, MITRE Caldera.

Impact, and References

Project Impact: Shifts SOC's from reactive assumed-breach models to proactive, continuous validation against modern identity threats.

- [1] R. Wright & J. Smith, "Identity as the New Perimeter..." IEEE TIFS, 2023.
- [2] K. Johnson & D. Clark, "Purple Teaming and Continuous Validation..." ACM Digital Threats, 2023.
- [3] B. Strom et al., "MITRE ATT&CK: Design and Philosophy," MITRE Corp, 2018.
- [4] S. O'Connor, "Overcoming Windows Event Forwarding Constraints..." Dig. Forensics Mag., 2024.

