Adversary Simulation Labs — Summary

Author: Velkris (Jared Perry)
Focus: Red Team Operations / Adversary Simulation
Environment: Controlled multi-VM lab based on MITRE ATT&CK TTPs
Purpose: Execute controlled simulations of real-world threat actor behaviors to validate detection coverage and strengthen red-team tradecraft.

Objective

Develop repeatable adversary-simulation exercises based on publicly documented APT techniques, evaluating telemetry visibility and defensive detection logic within a controlled lab environment.

Scenario Overview

Threat Actor	Mapped ATT&CK Techniques	Simulation Goals
APT28 (Fancy Bear)	Credential theft, scheduled task persistence, C2 over HTTP	Assess lateral movement and credential access visibility
APT29 (Cozy Bear)	Spearphishing, privilege escalation, data staging	Validate detection and log correlation for post-exploitation behavior

---

Methodology

- Selected TTPs from MITRE ATT&CK Enterprise matrix and OSINT reports
- Simulated **initial access**, **credential dumping**, and **C2 beaconing**
- Conducted **post-exploitation** with Rubeus and Mimikatz in sandboxed hosts
- Captured Sysmon, event, and network telemetry for blue-team analysis

---

Tools & Frameworks

C2 emulation (Mythic / Covenant) • Mimikatz • Rubeus • PowerView • BloodHound • Sysmon • MITRE ATT&CK Navigator

---

Findings

Category	Observation
Detection Visibility	Several TTPs (T1059.001, T1552.001) produced logs but lacked correlation rules.
Response Lag	EDR alerts triggered post-compromise due to limited real-time telemetry.
Technique Validation	Behavioral overlap confirmed between APT28/29 persistence and credential-abuse chains.

Recommendations

- Expand SIEM correlation for ATT&CK-mapped log sources (Sysmon, Event ID 4688, 7045).
- Conduct periodic adversary-simulation exercises focused on lateral movement and persistence tactics.
- Align red-team findings with blue-team rule tuning and threat-hunting priorities.

Outcome

Delivered detailed adversary-simulation reports highlighting detection coverage, response timelines, and attack-chain visibility.
Enhanced collaboration between offensive and defensive workflows through ATT&CK-aligned reporting and repeatable lab validation.

> This lab framework demonstrates operational understanding of adversary behavior, supporting continuous improvement of both red and blue team maturity.