CHANDIGARH UNIVERSITY, GHARUAN

Department of Computer Science and Engineering

INTERNSHIP REPORT

Submitted in Partial Fulfilment of the Requirements for the
Degree of
Bachelor of Engineering (B.E.) in Computer Science and Engineering

Internship Program (20 Sep-25 Dec):

Cybersecurity Internship Program – Shentinelix Sphere Pvt Ltd

Task 23

Attacking Active Directory, Post Exploitation, Intro to SIEM

Internship Report Submitted By:
Vikash Upadhyay

Table of Contents

Executive Summary

This combined report synthesizes learning from three TryHackMe modules: Attacking Active Directory, Post-Exploitation Basics, and Introduction to SIEM. Together these modules cover the attacker lifecycle from initial domain reconnaissance and exploitation (Kerberos abuses, BloodHound-driven pathfinding) through post-compromise consolidation (credential harvesting, lateral movement, persistence) to defender-side detection and response (SIEM concepts, log sources, alerting and triage). The integrated perspective emphasizes how offensive techniques manifest in telemetry and what defenders must collect and correlate to detect, investigate, and eradicate intrusions.

Completing these rooms provided both red-team skills (practical attack methods and tooling) and blue-team skills (SIEM alerts, triage playbooks, detection tuning). The hands-on labs strengthened my ability to (a) discover and exploit AD misconfigurations, (b) responsibly simulate post-exploit activities and map their forensic artifacts, and (c) translate attacker TTPs into SIEM detections and operational triage steps. This fusion of offensive and defensive knowledge prepares me to think like an adversary while building realistic detection and response controls.

Introduction

Modern enterprise compromises typically span identity systems, endpoint control, and telemetry ingestion gaps. Attack chains often begin with reconnaissance and credential abuse in Active Directory, progress through on-host post-exploitation that extracts credentials and establishes persistence, and become visible only if sufficient telemetry is ingested and correlated by a SIEM. To effectively detect and disrupt such chains, security practitioners need a holistic view: know the offensive techniques, what artifacts they leave on endpoints and the network, and how to encode those artifacts as SIEM detections and operational runbooks.

My learning workflow across the three modules was deliberately cyclical: execute a controlled offensive technique in a lab (e.g., Kerberoast or mimikatz) → capture the resulting host/network artifacts → identify the specific logs and fields a SIEM would see → draft detection queries and triage steps. This approach ensures that detection logic is grounded in realistic evidence and that red-team techniques are used to harden blue-team monitoring.

Overview of the Company

TryHackMe is an educational platform that provides accessible, hands-on cybersecurity labs and scenarios. Its rooms simulate realistic enterprise environments—vulnerable Active Directory domains, compromised endpoints, or SIEM consoles—so learners can practice both attacking and defending in a safe, repeatable setting. The platform pairs guided tasks with open-ended challenges, which is ideal for building procedural skillsets and investigative instincts.

In these modules, TryHackMe supplies AttackBoxes, curated artifacts (PCAPs, logs), and stepwise guidance that helps translate abstract TTP descriptions into concrete commands,

observable artifacts, and remediation recommendations. That close mapping between actions and telemetry is exactly what defenders need to build effective SIEM detections and response playbooks.

Description of Duties

My practical duties included: deploying lab environments (AttackBox or VM), performing AD enumeration and targeted Kerberos-based attacks (PowerView, BloodHound, Kerberoast/AS-REP tests), executing controlled post-exploitation tasks (mimikatz for credential dumping, creating/understanding Golden Tickets, lateral movement techniques), and practicing persistence techniques in a non-destructive manner. Parallel to offensive work, I identified and collected the corresponding host and network signals—Windows Event Logs, Sysmon events, and network flow/PCAP evidence—that reveal these actions.

On the defender side I ingested sample logs into a SIEM lab (or simulated queries), wrote detection queries and correlation rules for high-value TTPs, built small dashboards summarizing risky activity, and drafted triage/playbook steps (validate, enrich, contain, eradicate, recover). All activity was documented step-by-step so it can be reproduced, audited, and converted into runbooks for SOC analysts.

Acomplishments

• Successfully enumerated AD objects and found privileged attack paths using BloodHound and PowerView, demonstrating how small misconfigurations can lead to domain compromise.
• Performed safe post-exploitation demonstrations: credential extraction with mimikatz (sandboxed), simulated Golden Ticket behavior to understand Kerberos anomalies, and persistence testing to see what artifacts are left behind.
• Mapped offensive actions to concrete detection signals (e.g., LSA Secrets reads, unusual service creation, suspicious Ticket Granting Ticket patterns, anomalous process creation events) and authored SIEM queries and Snort/Suricata rule ideas to detect them.
• Produced concise remediation recommendations: tighten delegation, enforce managed service account hygiene, enable Sysmon and centralized logging, and tune SIEM alerts to reduce false positives.

Skills Learned

Technical: advanced AD enumeration and Kerberos attack techniques; BloodHound analysis to prioritize attack paths; use of mimikatz and safe Golden Ticket simulation; Sysmon/Event Log fields most relevant for credential and lateral movement detection; basic SIEM rule and dashboard creation (correlation queries, alert tuning).

Methodological: end-to-end evidence mapping—how a specific attack command translates into one or more log events and how those events should be correlated to form a high-fidelity alert. Improved ability to design SIEM detections that balance sensitivity and false positive rate.

Soft skills: professional incident documentation, writing triage/playbook steps, and communicating technical findings to operational teams.

Challenges Faced

• Environment constraints: some Kerberos or Golden Ticket behaviors require precise domain conditions; reproducing them reliably needs controlled lab setups.
• Tuning detections: converting forensic artifacts into SIEM rules requires careful field selection and thresholding to avoid alert fatigue while retaining coverage for real threats.
• Safe handling of powerful tools: working with credential extraction tools (mimikatz) and payload generators mandates strict sandboxing and strict no-networking policies to avoid accidental leakage or execution in production.

Conclusion

Combining offensive AD techniques, post-exploitation workflows, and SIEM detection practice yields the most practical defensive posture. Key recommendations:

1. **Telemetry First:** Deploy Sysmon with a tuned configuration, centralize Windows Event Logs and Sysmon into your SIEM, and ensure network telemetry (DNS, proxy, flow) is retained long enough for lateral movement investigations.
2. **Detect the TTPs:** Implement detections for LSA secret access, unusual ticket activity, anomalous service creation, new local admin additions, and suspicious process creation chains (powershell → cmd → rundll32, etc.). Use BloodHound-style graphs to prioritize defense on high-risk accounts and relationships.
3. **Harden Identity:** Enforce strong service account practices, reduce unconstrained delegation, rotate and limit service credentials, and apply Least Privilege.
4. **Playbooks & Practice:** Develop SOC playbooks mapping specific alerts to investigation steps (enrichment sources, containment actions), and run purple-team exercises to test detection coverage and tuning.

Acknowledgments

I would like to thank the team at Shentinelix Sphere Pvt. Ltd. for providing access to lab environments, learning resources, and a supportive environment that encouraged practical learning and skill development. Special thanks to the TryHackMe platform and the authors of the Research Methodology room for providing structured, hands-on lessons that significantly enhanced my research and problem- solving skills. Finally, I extend my gratitude to my peers and family for their continuous support and encouragement throughout the internship period.