# **Active Directory Pentest Lab — Summary**

**Author:** Velkris (Jared Perry)

Focus: Red Team / Adversary Simulation

**Environment:** Controlled multi-VM Active Directory domain

Purpose: Research and documentation for identity-based attack simulation and hardening

## **Objective**

Design and operate a safe, isolated Active Directory environment to explore enumeration, credential abuse, and privilege-escalation techniques while identifying detection and mitigation opportunities.

#### Lab Architecture

Component	Purpose
1 Domain Controller	Core AD services, Kerberos authentication
2 Windows Workstations	User endpoints for lateral movement and credential access
Kali Linux Host	Attacker node for enumeration, credential extraction, and exploitation

## **Key Activities**

- Enumeration: LDAP, SMB, and WinRM probing of domain users, groups, and SPNs.
- Credential Attacks: Kerberoast, AS-REP roasting, and constrained-delegation abuse.
- Privilege Escalation: Explored domain-admin pivot paths via BloodHound analysis.
- **Detection Validation:** Reviewed Windows event logs (4768/4769/4624) for visibility.

### **Tools Utilized**

# **Findings**

Category	Observation
Kerberos Hygiene	Multiple service accounts with weak SPNs vulnerable to roasting.
<b>Delegation Exposure</b>	Unconstrained delegation enabled unnecessary lateral access.
Logging Gaps	Limited Kerberos ticket and logon event visibility hindered detection.

## Recommendations

- Enforce least-privilege SPN assignments and rotate service-account passwords.
- Disable unconstrained delegation; restrict administrative logins via GPO.
- Expand event collection and correlation for ticket-based authentication.

### **Outcome**

Developed a reusable Active Directory Attack Simulation Lab with:

- Hardened Group Policy templates
- BloodHound path diagrams highlighting attack chains
- Remediation checklist for defender validation

This lab serves as a foundational reference for future adversary-simulation and detectionengineering projects.