Evaluating VLAN-Based Network Segmentation for Containing Credential-Based Lateral Movement in a Simulated Municipal Active Directory Environment

Master's Thesis Project Overview

Project Overview

This project evaluates whether VLAN-based network segmentation and least-privilege inter-VLAN firewall rules can reduce the success and progression of credential-based lateral movement in a simulated municipal Active Directory environment.

The study compares two configurations of the same virtual environment. The first serves as a relatively open baseline with limited east-west restrictions. The second separates systems into functional VLANs and uses OPNsense firewall rules to restrict communication according to least-privilege principles. Virtual machines, user accounts, credentials, operating-system versions, attack procedures, monitoring tools, and logging configurations remain as consistent as possible between the two conditions.

Research Question

How does VLAN-based network segmentation with least-privilege inter-VLAN firewall rules affect the success and progression of credential-based lateral movement in a simulated municipal Active Directory environment?

Supporting questions include:

- To what extent does segmentation reduce the number of network-reachable hosts, ports, and administrative services available from a compromised workstation?
- How does segmentation affect the highest stage of attack progression achieved during repeated credential-based lateral-movement trials?
- How do telemetry and detection outcomes differ between successful, blocked, and partially completed lateral-movement attempts?

Technical Environment

- Virtual Active Directory environment with Windows clients and servers
- OPNsense firewall for routing, VLANs, and least-privilege inter-VLAN policies
- Security Onion for centralized security monitoring and investigation
- Zeek and Suricata for network telemetry and detection
- Proxmox virtualization infrastructure
- Controlled attack system used only inside the isolated laboratory

Methodology

Standardized, harmless lateral-movement scenarios are repeated under both network conditions. The scenarios evaluate whether a compromised workstation can authenticate to another system, execute a remote command, or access a protected test resource.

The comparison measures:

- Attack success and highest stage of progression
- Reachable hosts, ports, and administrative services
- OPNsense firewall events
- Windows Security logs
- Security Onion telemetry and detections
- Detection outcomes and detection latency

A pilot test is completed before the main experiment to confirm that the attack procedures, monitoring tools, time synchronization, and environment reset process work consistently.

Research Foundation

The project uses peer-reviewed research, government publications, industry standards, and authoritative technical documentation. Research topics include network segmentation, Active Directory security, credential-based lateral movement, intrusion detection, virtual cybersecurity laboratories, and security challenges in smaller or resource-constrained organizations.

Research Boundaries

All testing occurs within an isolated virtual laboratory created for education and research. The project does not use a production network belonging to a real municipality and does not involve citizen information, confidential organizational documents, live organizational credentials, surveys, interviews, focus groups, or other human participants.

Project Value

The project is intended to provide practical evidence about whether accessible technologies such as VLANs, OPNsense, and open-source monitoring tools can provide measurable containment and visibility benefits in a resource-constrained environment.

It also distinguishes among blocking an attack, recording telemetry, and producing a meaningful security detection. These outcomes are measured separately so that containment and detection are not treated as the same result.

The findings may provide a practical example of how functional segmentation can be designed and evaluated without relying on expensive enterprise security platforms.