📑 Security Hardening & Audit Report

Project: Cloud-Based Identity Management & Windows Server Hardening

Auditor: Zekrima Rizka

Date: 18 Februari 2026

Status: ✅ Completed

---

1. Executive Summary

Laporan ini merinci langkah-langkah pengerasan keamanan (*hardening*) yang diterapkan pada Windows Server 2019 Core yang dikonfigurasi sebagai Domain Controller. Tujuan utama adalah untuk mengurangi *attack surface*, mengamankan manajemen identitas, dan memastikan kepatuhan terhadap standar keamanan dasar (NIST/CIS).

---

2. Technical Environment

- **Operating System:** Windows Server 2019 Core (Version 1809)
- **Role:** Active Directory Domain Controller (AD DS)
- **Host Environment:** Ubuntu 22.04 LTS (KVM/QEMU)
- **Management Protocol:** OpenSSH (Port 22) - Encrypted CLI Access

---

3. Implementation Checklist & Risk Mitigation

Berikut adalah rincian kontrol keamanan yang telah diimplementasikan:

Control Area	Implementation Action	Risk Mitigated
System Footprint	Deployment of **Server Core** (No-GUI).	Mengurangi kerentanan pada komponen UI dan meminimalkan beban *patching*.
Network Security	Disabled **SMBv1** & Legacy Protocols.	Mencegah serangan *lateral movement* dan eksploitasi lawas seperti WannaCry/EternalBlue.
Identity Protection	Configured **Account Lockout Policy** (5 attempts).	Melindungi akun administratif dari serangan *Brute Force* dan *Dictionary Attack*.
Access Control	**SSH Host-Restricted** Inbound Rule.	Membatasi akses manajemen hanya dari IP Host tertentu, mencegah akses tidak sah dari jaringan luar.
Endpoint Defense	Active **Host Firewall** for all profiles.	Menutup semua port yang tidak diperlukan untuk layanan Domain Controller.
Accountability	Enhanced **Logon Audit Policy** (Success/Failure).	Memastikan adanya *audit trail* untuk setiap percobaan akses ke sistem.

---

4. Security Configuration Details (Proof of Work)

A. Password & Lockout Policy

Kebijakan yang diterapkan memastikan bahwa penyerang tidak dapat mencoba kata sandi tanpa batas waktu.

- **Threshold:** 5 invalid logon attempts.

- **Observation Window:** 30 minutes.

B. Legal Warning Banner

Setiap percobaan akses melalui SSH atau konsol akan menampilkan peringatan hukum:

> *"WARNING: Authorized Access Only. All activities are monitored and recorded."*

C. Logging & Monitoring

Kebijakan audit ditingkatkan untuk mencatat kejadian berikut ke dalam Event Viewer:

- Semua keberhasilan dan kegagalan login.
- Perubahan pada kebijakan keamanan sistem.