Dealership IT Infrastructure Simulation Project Summary

# Executive Summary

This project, authored by Christian Leep, simulates a complete IT infrastructure deployment for a fictional automotive dealership. The goal was to design, build, and configure an enterprise-ready environment that mirrors the real-world responsibilities of a Systems Administrator or IT Support Specialist. The project demonstrates end-to-end capabilities including Active Directory Domain Services (AD DS), DNS, DHCP, Group Policy, security hardening, file and print services, remote administration, auditing, and more — all implemented within a virtualized lab environment using VirtualBox.

# Introduction

The automotive dealership industry relies on reliable, secure, and scalable IT infrastructure to support daily operations, from sales and service to administrative workflows. This project was developed to simulate those exact needs and showcase the technical expertise required to build and manage such an environment. By building a domain from scratch, configuring core network services, applying security policies, and enabling centralized management, this project reflects real-world skills used in enterprise IT environments.

# Project Objectives

- Deploy a Windows Server 2022-based domain controller with AD DS, DNS, and DHCP.  
- Create a secure, scalable domain structure with Organizational Units (OUs), users, and security groups.  
- Implement Group Policy Objects (GPOs) to enforce organizational standards.  
- Configure file and printer sharing with access control and drive mapping.  
- Enable remote management and administrative access through secure RDP policies.  
- Implement auditing and monitoring policies for accountability and security.  
- Simulate real-world ticket resolution workflows and IT support processes.

# Environment Setup

The project environment was built entirely within Oracle VirtualBox to replicate a multi-machine enterprise setup. It consisted of the following virtual machines:  
- Domain Controller (Dealership-DC) – Hosts AD DS, DNS, DHCP, Group Policy, and time synchronization services.  
- Management Server (MGMT-SRV) – Used for remote administration, Group Policy management, file sharing, and RDP access.  
- Client Machines (Sales-PC, Service-PC) – Domain-joined Windows 11 workstations representing dealership staff endpoints.  
  
The network was configured with an internal subnet (192.168.1.0/24) for domain services and a NAT interface for internet access.

# Step-by-Step Infrastructure Deployment

1. Domain Controller Configuration – Installed AD DS, DNS, and DHCP roles, configured static IP (192.168.1.10), and created the root domain `dealership.local`.  
2. DNS Configuration – Created forward and reverse lookup zones, enabled secure dynamic updates, added forwarders, and configured scavenging.  
3. DHCP Setup – Authorized the DHCP server, created scopes (192.168.1.100–200), set default gateway and DNS options, and configured DNS update integration.  
4. Organizational Units and Structure – Created OUs for `Servers`, `Workstations`, `Users`, and `Groups` to logically separate and manage domain objects.  
5. User and Group Management – Created accounts (`SalesRep01`, `ServiceRep01`) and added them to security groups (`SalesDept`, `ServiceDept`) to enforce access control.  
6. Group Policy Management – Implemented password complexity, lockout policies, audit logging, drive mapping, and RDP restrictions.  
7. File and Printer Sharing – Created department-specific shares (`Sales`, `Service`), configured SMB permissions, and deployed mapped drives via GPO.  
8. Remote Desktop Access Control – Enabled RDP, configured firewall rules, and restricted access to administrative groups using Group Policy.  
9. Auditing and Security Policies – Enabled logon/logoff, account lockout, and Kerberos event auditing. Configured custom event log views for monitoring.  
10. Testing and Validation – Verified DHCP leases, DNS name resolution, GPO application (`gpresult /r`), and RDP connectivity from MGMT-SRV to client endpoints.

# Security and Hardening Measures

Security was a core focus throughout the project. Key controls implemented include:  
- Password Policy: Enforced complexity, history, and expiration.  
- Account Lockout Policy: Throttled brute-force attempts.  
- Audit Policies: Logged critical authentication events and privileged activity.  
- RDP Restrictions: Limited remote access to domain-admin groups only.  
- NTFS & SMB Permissions: Implemented least privilege on file shares.  
- DNS Scavenging: Prevented stale records from accumulating.  
- Time Synchronization: Ensured Kerberos ticket accuracy and event correlation.

# Results and Outcomes

By the end of this project, a fully functional, secure, and realistic enterprise network environment was successfully deployed. The system demonstrated core infrastructure services, centralized policy enforcement, controlled remote access, automated DNS/DHCP integration, and real-world support capabilities. The environment is fully extensible for future services like SMTP email simulation, VPN configuration, ticketing systems, and remote monitoring.

# Lessons Learned & Takeaways

Through this project, I gained a deeper understanding of end-to-end enterprise network design and deployment. Key lessons included:  
- The importance of planning and documenting network architecture before implementation.  
- How DNS, DHCP, and AD DS interconnect to create a functional identity infrastructure.  
- Real-world considerations for Group Policy structuring, OU hierarchy, and delegation.  
- The value of security-first design, including account policies, audit logging, and RDP restrictions.  
- How infrastructure projects can be presented as business-focused solutions, not just technical builds.  
  
This project now serves as a strong portfolio example of my ability to design, implement, and manage Windows-based enterprise networks.