SYNTHETIC DEMONSTRATION / NO CUSTOMER DATA

SECURITY ASSESSMENT REPORT

Security Assessment

Active Directory Health Report

corp.acmeinc.com

Assessment Date: 2026-03-15

Overall Risk: High Risk (65/100)

SYNTHETIC DEMONSTRATION REPORT

Sample values only. No customer or production environment is represented.

Executive Summary

65	18	3	8	2/5
OVERALL SCORE	TOTAL FINDINGS	CRITICAL	HIGH	MATURITY LEVEL

This report presents the findings from an automated Active Directory security assessment of **corp.acmeinc.com** (ACMEINC), conducted on 2026-03-15 using PingCastle v3.5.0.37. The overall risk score is **65/100**, rated as **High Risk**. A total of **18** security findings were identified, of which **3** are critical severity.

Severity Scale: Critical 30+ pts High 15-29 pts Medium 5-14 pts Low 1-4 pts

Top Priority Findings

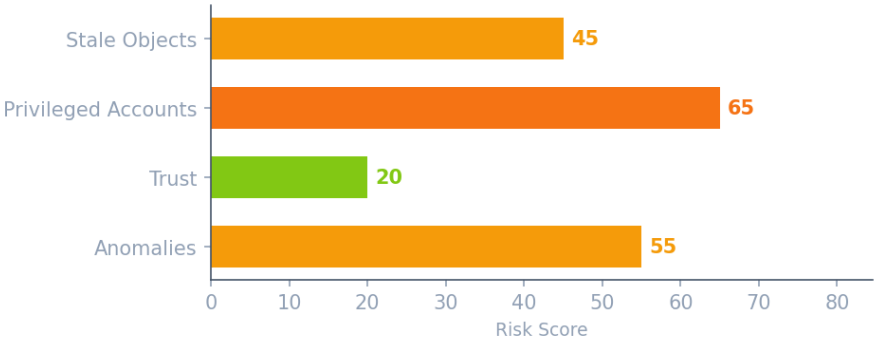
FINDING	CATEGORY	SCORE	SEVERITY
KRBTGT Account Password Not Changed	Anomalies	40	Critical
Too Many Domain Admins	Privileged Accounts	35	Critical
Unconstrained Delegation Configured	Privileged Accounts	30	Critical
SMBv1 Still Enabled	Anomalies	25	High
Windows Server 2008/R2 Systems Detected	Stale Objects	20	High

Risk Dashboard

Overall Risk Score

Finding Severity Distribution

Category Breakdown



Security Maturity Level

Level 1	**Level 2**	Level 3	Level 4	Level 5

The domain is currently at **Maturity Level 2** out of 5. Significant improvements are needed to reach a baseline security posture.

Domain Information

DOMAIN	**corp.acmeinc.com**
NETBIOS NAME	**ACMEINC**
DOMAIN FUNCTIONAL LEVEL	**Windows Server 2016**
FOREST FUNCTIONAL LEVEL	**Windows Server 2016**
DOMAIN CONTROLLERS	**3**

ACTIVE USERS	1247
ACTIVE COMPUTERS	892
ASSESSMENT DATE	2026-03-15

DEMONSTRATION CONTEXT

How to read this sample

This report is a synthetic example created to demonstrate report structure, prioritization, and remediation planning. The domain, accounts, dates, scores, and findings are sample values. They do not document work for ACME or any customer.

What the artifact demonstrates

- Turning technical findings into a concise executive summary
- Separating severity, business context, and remediation effort
- Organizing corrective work into quick-win, short-term, and long-term phases
- Producing an inspectable handoff record without exposing private client data

Detailed Findings

Anomalies (8 findings, 130 points)

FINDING	DESCRIPTION	SCORE	SEVERITY
KRBTGT Account Password Not Changed A-Krbtgt	The KRBTGT account password has not been rotated recently, leaving the domain vulnerable to Golden Ticket attacks.	40	Critical
SMBv1 Still Enabled A-SMB1	SMBv1 is enabled, which is vulnerable to EternalBlue and other critical exploits (WannaCry, NotPetya).	25	High
Print Spooler Running on Domain Controllers A-DC-Spooler	The print spooler service is running on DCs, which can be exploited for privilege escalation (PrintNightmare).	15	High
LAPS Not Deployed A-LAPS-Not-Installed	Local Administrator Password Solution is not deployed, meaning local admin passwords may be shared across machines.	15	High
PowerShell Logging Not Enabled A-AuditPowershell	PowerShell script execution is not being logged, making it easy for attackers to run malicious scripts undetected.	10	Medium
Pre-Windows 2000 Compatible Access Group Has Members A-PreWin2000Other	This legacy group grants anonymous access to AD data, potentially exposing sensitive information.	10	Medium
SYSVOL Using Legacy NTFRS Replication A-NTFRSOnSysvol	SYSVOL replication is using the deprecated NTFRS instead of DFS-R, which is less reliable and no longer supported.	10	Medium
Minimum Password Length Too Short A-MinPwdLen	The domain password policy allows passwords shorter than recommended, increasing brute-force risk.	5	Medium

Privileged Accounts (6 findings, 110 points)

FINDING	DESCRIPTION	SCORE	SEVERITY
Too Many Domain Admins P-AdminNum	An excessive number of accounts have Domain Admin privileges, expanding the attack surface.	35	Critical
Unconstrained Delegation Configured P-Delegated	Servers with unconstrained delegation can impersonate any user, a major privilege escalation vector.	30	Critical
Service Accounts in Domain Admins P-ServiceDomainAdmin	Service accounts have been added to the Domain Admins group, granting excessive privileges.	20	High
Admin Account Passwords Are Too Old P-AdminPwdTooOld	Some admin account passwords have not been changed in an extended period.	15	High
Protected Users Group Not Utilized P-ProtectedUsers	Admin accounts are not in the Protected Users group, missing additional Kerberos protections.	5	Medium
AD Recycle Bin Not Enabled P-RecycleBin	The AD Recycle Bin is not enabled, meaning accidentally deleted objects cannot be easily recovered.	5	Medium

Stale Objects (3 findings, 45 points)

FINDING	DESCRIPTION	SCORE	SEVERITY
Windows Server 2008/R2 Systems Detected S-OS-2008	End-of-support Server 2008 systems are present in the domain.	20	High
Accounts with Non-Expiring Passwords S-PwdNeverExpires	User accounts are configured with passwords that never expire, increasing long-term compromise risk.	15	High
Stale/Inactive User Accounts S-Inactive	User accounts that have not logged in for an extended period remain enabled.	10	Medium

Trust (1 findings, 20 points)

FINDING	DESCRIPTION	SCORE	SEVERITY
NTLM Authentication Still Allowed T-AlgsNTLM	NTLM authentication is permitted, which is weaker than Kerberos and vulnerable to relay attacks.	20	High

Remediation Roadmap

Findings are prioritized into three phases based on implementation effort and risk reduction impact.

Quick Wins (0-30 days) - 8 items

FINDING	REMEDIATION	SCORE	EFFORT
Print Spooler Running on Domain Controllers	Disable the Print Spooler service on all domain controllers.	15	low
Admin Account Passwords Are Too Old	Enforce regular password rotation for all privileged accounts.	15	low
PowerShell Logging Not Enabled	Enable PowerShell Script Block Logging and Module Logging via GPO.	10	low
Pre-Windows 2000 Compatible Access Group Has Members	Remove all members from the Pre-Windows 2000 Compatible Access group.	10	low
Stale/Inactive User Accounts	Disable or remove accounts inactive for 90+ days.	10	low
Minimum Password Length Too Short	Set minimum password length to at least 12 characters via Default Domain Policy.	5	low
Protected Users Group Not Utilized	Add privileged accounts to the Protected Users security group.	5	low
AD Recycle Bin Not Enabled	Enable the Active Directory Recycle Bin feature.	5	low

Short-Term (30-90 days) - 6 items

FINDING	REMEDIATION	SCORE	EFFORT
KRBTGT Account Password Not Changed	Reset the KRBTGT password twice (with replication interval between resets).	40	medium
Too Many Domain Admins	Review and reduce Domain Admin membership to the minimum required.	35	medium
SMBv1 Still Enabled	Disable SMBv1 on all systems via GPO and verify no legacy dependencies.	25	medium
Service Accounts in Domain Admins	Remove service accounts from Domain Admins; grant only necessary permissions.	20	medium
LAPS Not Deployed	Deploy Microsoft LAPS or Windows LAPS to manage local administrator passwords.	15	medium
Accounts with Non-Expiring Passwords	Review accounts with non-expiring passwords; enforce expiration or use managed service accounts.	15	medium

Long-Term (90+ days) - 4 items

FINDING	REMEDIATION	SCORE	EFFORT
Unconstrained Delegation Configured	Switch to constrained delegation or resource-based constrained delegation.	30	high
Windows Server 2008/R2 Systems Detected	Migrate workloads from Server 2008/R2 to supported versions.	20	high
NTLM Authentication Still Allowed	Progressively restrict NTLM; audit usage first, then block where possible.	20	high
SYSVOL Using Legacy NTFRS Replication	Migrate SYSVOL replication from NTFRS to DFS-R.	10	high