FINANCIAL SERVICES / AD CRITICAL

Help Desk Login to Domain Admin in Four Steps

CVSS 9.1 | Full attack path documented

01 Engagement Overview

A financial services firm running Active Directory as its core identity backbone engaged DivIHN for an internal penetration test, treating help desk-tier access as a low-privilege starting point with no expected path to domain compromise.

- **Scope:** Internal AD environment, group policy configuration, delegation settings, privileged group membership
- **Approach:** Assumed-breach simulation starting from a standard help desk technician account
- **Baseline:** SIEM and endpoint monitoring in place, no prior domain-admin-path findings

02 Technical Discovery

Starting from a help desk technician's standard credentials, DivIHN's team mapped a four-hop path to full domain compromise, each hop enabled by a misconfiguration invisible to standard access reviews.

- **Hop 1:** Help desk account held edit rights on a GPO linked to a workstation OU, left over from a prior delegation task
- **Hop 2:** Modified the GPO to push a malicious scheduled task, executing as SYSTEM on a Tier 1 support admin's workstation
- **Hop 3:** Harvested the Tier 1 admin's credentials, which held unconstrained delegation rights on a service account
- **Hop 4:** Used that delegation trust to impersonate a domain controller session and escalate to Domain Admin
- No hop resembled a known exploit signature, so no alert fired along the chain

03 Risk & Business Impact

The finding scored CVSS 9.1, Critical, reflecting a privilege escalation path that required no exploit code, only chained misconfigurations across GPO delegation and Kerberos delegation settings.

- Domain Admin access in a financial services AD environment means unrestricted access to core banking systems, customer PII, and audit logging infrastructure itself
- The chain evaded detection because each step was a legitimate administrative action taken with valid, if over-permissioned, credentials
- **Regulatory exposure:** this class of finding falls squarely under FFIEC and GLBA expectations for privileged access controls and directly informs SOC 2 and PCI DSS scoping

04 Remediation & Outcome

DivIHN worked with the client's IAM team to remove the excess delegation and close the detection gap that let the chain run silently.

- Removed help desk account's GPO edit rights, scoped to the original one-time task
- Converted the exposed service account to constrained delegation (Kerberos)
- Enabled advanced auditing on GPO and delegation changes, wired to SIEM alerting
- Instituted a quarterly AD privilege and delegation review alongside existing access reviews