

Executive Summary

This assessment documents an intentionally misconfigured Active Directory environment designed to demonstrate Kerberoasting feasibility under insecure service account configurations. A user-based service account with a registered SPN and non-expiring password was introduced to simulate common enterprise misconfigurations. Kerberos service ticket issuance was validated, confirming exposure to offline password cracking attacks. This report contrasts directly with the hardened baseline documented in Report 1.

TDNA Assessment – Report 2: Vulnerable Active Directory Environment

This report documents a purposefully misconfigured Active Directory environment designed to demonstrate Kerberoasting feasibility under insecure service account configurations. The environment contrasts directly with Report 1, where Kerberoasting was not possible due to hardened controls.

Objective

Demonstrate Kerberoasting viability by introducing a controlled misconfiguration and documenting evidence of Kerberos service ticket issuance suitable for offline password cracking.

Intentional Misconfiguration Summary

- Service account: svc_sql
- SPN registered to user-controlled account
- Password never expires
- Legacy RC4 encryption allowed
- Result: Kerberoastable TGS issued

Attack Validation

A standard domain user successfully requested a Kerberos service ticket for the MSSQLSvc service. The resulting ticket was cached locally and confirmed to use RC4-HMAC encryption, meeting Kerberoasting preconditions.

Evidence Collected

- setspn enumeration confirmed MSSQLSvc SPN registration
- klist confirmed cached service ticket
- Windows Security Event ID 4769 logged service ticket issuance
- Ticket encryption type confirmed vulnerable configuration

Conclusion

Kerberoasting was successfully enabled in this environment due to intentional service account misconfiguration. This demonstrates how legacy encryption settings and improper service

account management directly introduce credential exposure risk. The contrast with Report 1 highlights the effectiveness of proper Kerberos hardening controls.