



INTERNAL NETWORK / ACTIVE DIRECTORY - SYNTHETIC SAMPLE

Internal Network & Active Directory

From a foothold to the boundary that actually holds.

A fictional lab, not a client assessment. All identities, hosts, transcripts, paths and outcomes are synthetic. No production network was tested to create this sample. It illustrates the deliverable and the limits of each conclusion.

6 findings / 3 illustrated paths

2 High / 3 Medium / 1 Low

Evidence, controls, cleanup and retest acceptance criteria

PXLSec / PXLSecurity LTD.

29 October 2026 / v1.0

SECTION READ FIRST

Document control & contents

Public marketing sample. No real client, production secret or executed attack is represented.

Document	PXLSec-AD-SAMPLE / v1.0
Classification	Public synthetic sample; no client data
Environment	EXAMPLE.TEST / TEST-NET 192.0.2.0/24
Evidence status	Every evidence block is invented for illustration.
Retest status	NOT RETESTED

Section	Content	Page
01	Executive summary	3
02	Scope and starting positions	4
03	Method, coverage and safety	5
03A	Course of the assessment	6
04	Findings and technical evidence	9
05	Remediation sequence	22
06	Retest and closure	23
APPENDIX	Evidence, cleanup and references	24

SECTION 01

Executive summary

The same network can expose one privilege path and still deny another.

6	9	0
illustrative findings	narrative stages	real clients

The fictional lab contains two High, three Medium and one Low finding. A recoverable privileged service identity permits a controlled domain credential-replication demonstration. Excessive group delegation reaches one member server. A separate relay exercise establishes only a bounded LDAP read: the protected write is denied.

The chronological account records discovery, credential exposure, Kerberoasting and single-account replication, then the remaining scoped checks. Shared-file secrets, anonymous enumeration and a pre-authentication exception have independent prerequisites and deliberately limited outcomes. No finding is promoted to a domain compromise because a tool listed it.

Decisions to make first

- 1 Remove unnecessary domain and group-control privilege; preserve the service dependencies.
- 2 Retire exposed identities and correct the actual authentication paths, including signing requirements.
- 3 Repeat each original path with its controls; a settings screenshot alone is not closure.

Positive control. Protected LDAP writes, anonymous file reads and refreshed-token access after cleanup are denied in the sample. Those boundaries remain part of the result.

SECTION 02

Scope and starting positions

Every path is tied to its own account, host and allowed action.

Domain	EXAMPLE.TEST (fictional)
Targets	DC-01 192.0.2.10; FILE-01 192.0.2.20; APP-01 192.0.2.30; WS-LAB 192.0.2.40; SQL-01 192.0.2.50
Starting identities	Anonymous on-network host; ordinary alice; delegated support user; owned test principal.
Test authority	A real engagement requires a signed target list and rules of engagement. None was executed for this sample.
Excluded	Cloud identity, trusts, AD CS exploitation, OT, phishing, password spraying, bulk credential replication, destructive tests and unrelated hosts.

Operational controls

- Agree the source addresses, credentials, time windows, escalation contact and stop conditions before active checks.
- Use dedicated test objects and reversible membership changes; avoid live-user authentication coercion outside explicit scope.
- Record exclusions as untested, not secure. Approval to read one container does not authorise a full directory dump.

SECTION 03

Method, coverage and safety

Discover a relationship, validate the transition, then record both success and denial.

Area	Sample coverage	Boundary
Kerberos	AD-01, AD-06	One recovered lab secret; one unsuccessful recovery.
LDAP / NTLM	AD-02	Bind/read accepted, protected write denied.
Delegation / ACL	AD-03	One reversible group-to-host path.
Shares / secrets	AD-04, AD-05	Scoped script and account names only.
AD CS / trusts / cloud	Not exercised	No security conclusion.

Evidence and severity

Each evidence ID identifies a specific observation and its principal. A path is not validated by a graph edge alone. Severity is contextual to the stated lab access and demonstrated operation. Illustrative CVSS v3.1 Base scores are calculated from the full vectors in each finding. Report severity is a contextual priority and can differ from the CVSS Base band.

Detection and safety

A real handoff correlates the ticket, bind, logon and group-change evidence with available defender telemetry. This sample does not fabricate SIEM alerts, EDR evasion or detection times. Availability and identity lockout limits take precedence over proving a longer path.

SECTION 03A

Course of the assessment

Discovery, validation, exploitation and the next decision.

Illustrative reconstruction. The first-person account below explains the sample findings in chronological order. It is not a record of a newly performed customer test. Supplied access and independent checks are identified explicitly.

01 / We scanned the agreed internal range

We began from the approved on-network test host and performed host discovery and a scoped service scan. The results identified DC-01, FILE-01, SQL-01 and APP-01 and exposed the expected SMB, LDAP and Kerberos services. We correlated service responses with DNS and the agreed target list before continuing. The client-provided ordinary account `alice` was available for the authenticated phase; it was not obtained by the scan.

Evidence reference: N-01: synthetic discovery/service inventory; scope

02 / Anonymous enumeration disclosed account names

Before using `alice`, we tested the unauthenticated SMB/RPC boundary on FILE-01. The account-name query returned `alice`, `bob` and `svc_lab_backup`. Anonymous access to protected file content was denied. We recorded the information disclosure, then switched explicitly to the provided ordinary account for share review. No password spraying or guessed account takeover was needed for that transition.

Evidence reference: AD-05 / AD05-E1-E3

03 / A deployment share exposed a working service credential

As `alice`, we enumerated the readable shares and inspected the scoped LabDeploy script on FILE-01. It contained the synthetic password for `svc_lab_backup`. We authenticated with that identity to confirm the password was current, but an administrator-only operation was denied. We had gained a valid service identity, not Domain Admin. We did not open backup archives or test password reuse on unrelated systems.

Evidence reference: AD-04 / AD04-E1-E3

SECTION 03A / 2

Course of the assessment

Discovery, validation, exploitation and the next decision.

04 / Directory enumeration revealed the next escalation opportunity

Using the authenticated domain access, we examined service principals, group membership and delegation. svc_lab_sql had an MSSQLSvc SPN and unnecessary Domain Admin membership. That combination made its service ticket a high-value offline target. We requested only the permitted ticket and recorded its principal and the privilege that would become available if password recovery succeeded.

Evidence reference: AD-01 / AD01-E1

05 / Kerberoasting recovered the privileged lab password

We tested the captured service ticket within the agreed offline budget. The service password was recovered. We authenticated as svc_lab_sql and confirmed its effective domain privilege with the agreed control operation; the same operation as alice had been denied. The escalation therefore depended on both successful recovery and excessive membership, not merely the existence of an SPN.

Evidence reference: AD-01 / AD01-E2-E3

06 / We demonstrated access to a lab domain credential hash

To confirm the credential impact, we continued with the expressly authorised replication check against DC-01. Using the recovered privileged identity, we requested replication data for one dedicated canary account only. The result contained that account NT hash, proving credential-replication impact. The hash is withheld from this public sample. We did not collect all domain hashes, extract krbtgt material, crack the canary hash or use it for a further logon.

Evidence reference: AD-01 / AD01-E4: synthetic single-account replication

SECTION 03A / 3

Course of the assessment

Discovery, validation, exploitation and the next decision.

07 / We continued with delegation and server access

After proving the domain escalation, we returned to the separately provided support-user context to avoid masking weaker controls with Domain Admin rights. Its delegation allowed changes to LAB-App-Admins, mapped to local administration on APP-01. We made the reversible membership change, obtained a fresh session and confirmed one administrator-only sentinel on APP-01. We then restored membership and verified denial with a refreshed session.

Evidence reference: AD-03 / AD03-E1-E3

08 / Relay and AS-REP checks produced different outcomes

We next exercised the separately agreed machine-authentication relay. LDAP accepted the relayed identity and allowed the scoped read, but denied the protected write. Finally, an account with pre-authentication disabled returned AS-REP material; the bounded recovery attempt failed. Neither test supplied the earlier Domain Admin access. Recording both the successful read and the failed continuations explains what we actually achieved in this lab story.

Evidence reference: AD-02 / AD02-E1-E3; AD-06 / AD06-E1-E3

09 / We closed the exercise and handed over the evidence

We ended the sessions, verified the membership rollback and documented the affected identities for client-owned rotation. The evidence register ties discovery, exposed credentials, service-ticket recovery, single-account replication and server-access confirmation to their findings. No persistence was added. No remediation was retested in this sample. The whole chronology is an expanded fictional lab reconstruction, not a record of newly executed client activity.

Evidence reference: Evidence register; cleanup; retest status

SECTION 04

Findings and technical evidence

Six independent findings. Every evidence block below is synthetic.

ID	Finding	Severity	CVSS 3.1
AD-03	Delegated group write reaches one member server	High	8.8
AD-01	A recoverable service password grants domain-level privilege	High	7.5
AD-06	A lab account has Kerberos pre-authentication disabled	Medium	5.3
AD-04	A readable deployment script exposes a service identity	Medium	4.3
AD-02	Relayed authentication permits a bounded LDAP read	Medium	3.1
AD-05	Null-session enumeration discloses lab account names	Low	5.3

All finding statuses are **Illustrative / NOT RETESTED**. Synthetic success is not evidence that an actual organisation is compromised.

SECTION AD-03

Delegated group write reaches one member server

Synthetic evidence; no real assessment was executed.

Report severity	HIGH
CVSS v3.1 Base	8.8 / High (illustrative Base) CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H Existing delegated user; effective administration of one member server.
Component	LAB-App-Admins group ACL and its local-administrator assignment on APP-01.
Starting access	An ordinary user inheriting the fictional support delegation; one approved reversible group change.
ATT&CK	T1098.007
Status	Illustrative / NOT RETESTED

Description

A support group can modify membership of LAB-App-Admins, which is mapped to local Administrators on one lab application server. The tester adds only a dedicated test principal, obtains a fresh logon and validates a harmless administrator-only sentinel. Removing the membership and refreshing the token returns the sentinel to denied.

SYNTHETIC EVIDENCE / NOT A CAPTURED SESSION

```
AD03-E1 | Support-L1 -> WriteMembers -> LAB-App-Admins
AD03-E1 | LAB-App-Admins -> local Administrators -> APP-01
AD03-E2 | before change, test principal sentinel: denied
AD03-E2 | after approved membership + fresh logon: accepted
AD03-E3 | membership restored + fresh logon: denied
SCOPE   | no DC access or other member-server checks
```

Illustrated impact and stop point

Administrative authority on APP-01 is illustrated. Domain-controller administration, lateral reach to other servers and persistence are not established. Cached tokens must be considered during remediation.

SECTION AD-03 / CONTINUED

Reproduction, remediation and verification

Root cause

A delegated administration edge crosses an unintended privilege boundary. Group membership, nested membership and effective local rights must be considered together, not as isolated configuration rows.

Reproduction approach

- 1 Record the starting user, inherited ACL and the group-to-host assignment.
- 2 Confirm the test principal cannot perform the agreed administrator-only operation before the change.
- 3 Apply the approved membership change, obtain a fresh token and run only the harmless sentinel.
- 4 Remove the membership, verify the restored ACL state and repeat with a new logon.

Remediation

- Remove the unnecessary membership-write delegation and review inherited/nested group paths.
- Restrict privileged group administration and refresh or revoke affected sessions according to the incident plan.

Retest acceptance criteria - not performed

The original support user cannot change the privileged membership; an authorised administrator can; the fresh-token sentinel remains denied for the test principal.

Handoff. A real finding includes the exact principal, timestamps, configuration, response and secure evidence reference. Never paste a recovered password into a broadly distributed report.

SECTION AD-01

A recoverable service password grants domain-level privilege

Synthetic evidence; no real assessment was executed.

Report severity	HIGH
CVSS v3.1 Base	7.5 / High (illustrative Base) CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H Offline recovery is required; the recovered identity has domain-wide authority.
Component	svc_lab_sql, its SPN, password lifecycle and privileged group membership.
Starting access	Ordinary EXAMPLE.TEST user; access to Kerberos and the authorised lab ticket.
ATT&CK	T1558.003
Status	Illustrative / NOT RETESTED

Description

The fictional service account combines an SPN, a deliberately recoverable lab password and Domain Admin membership. An ordinary account can request its service ticket. A bounded offline exercise recovers the lab secret, then a privilege check confirms the service identity. A separately authorised, single-canary replication check then illustrates access to one domain NT hash. These are three separate observations: ticket availability, successful recovery and effective privilege.

SYNTHETIC EVIDENCE / NOT A CAPTURED SESSION

```
AD01-E1 | principal: svc_lab_sql | SPN: MSSQLSvc/sql-01.example.test
AD01-E1 | membership: Domain Admins (fictional lab)
AD01-E2 | bounded offline result: lab secret recovered; value withheld
AD01-E3 | authenticated identity: EXAMPLE\svc_lab_sql
AD01-E3 | agreed privileged read probe: accepted
AD01-E4 | authorised single-account replication: lab_canary NT hash [WITHHELD]
CONTROL | identical privileged probe as EXAMPLE\alice: denied
```

Illustrated impact and stop point

Domain-level authority is illustrated for this lab identity. Credential recovery is conditional on the actual secret and test budget. A separately authorised replication check returned the NT hash of one fictional canary account (AD01-E4), with the value withheld. No bulk domain dump, krbtgt collection, hash reuse or persistence is included.

SECTION AD-01 / CONTINUED

Reproduction, remediation and verification

Root cause

A service identity has both unnecessary domain-wide authority and a password that fails the agreed resistance requirement. An SPN alone is normal and is not this finding.

Reproduction approach

- 1 Confirm the test user, permitted service principal and effective group membership.
- 2 Collect only the agreed service ticket; record the requesting account and scope.
- 3 Perform the bounded offline test; keep the recovered secret out of the distributed PDF.
- 4 Authenticate as the lab service identity, compare the privileged probe with the ordinary-user control, then perform only the separately authorised single-canary replication check.

Remediation

- Remove unnecessary Domain Admin membership and verify service dependencies before changing rights.
- Use a supported managed service identity or a strong, rotated random secret; retire the exposed lab equivalent.

Retest acceptance criteria - not performed

The service still works with least privilege; the old secret is rejected; ordinary users cannot reach the privileged sentinel. A failed crack alone does not prove all service identities safe.

Handoff. A real finding includes the exact principal, timestamps, configuration, response and secure evidence reference. Never paste a recovered password into a broadly distributed report.

SECTION AD-06

A lab account has Kerberos pre-authentication disabled

Synthetic evidence; no real assessment was executed.

Report severity	MEDIUM
CVSS v3.1 Base	5.3 / Medium (illustrative Base) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Pre-authentication response exposed; no recovered password or logon.
Component	Pre-authentication setting on svc_lab_legacy.
Starting access	Knowledge of the scoped lab account and access to the domain Kerberos endpoint.
ATT&CK	T1558.004
Status	Illustrative / NOT RETESTED

Description

The scoped account returns a roastable AS response without pre-authentication. The bounded offline test does not recover its password. The exposure is still a control weakness, but a password recovery, authenticated foothold or privileged continuation is explicitly not claimed.

SYNTHETIC EVIDENCE / NOT A CAPTURED SESSION

```
AD06-E1 | account: svc_lab_legacy | pre-authentication required: no
AD06-E2 | AS response obtained within authorised lab scope
AD06-E3 | bounded offline test: no password recovered
CONTROL | otherwise equivalent protected account: pre-auth required
STOP    | no authenticated access attributed to this finding
```

Illustrated impact and stop point

The account permits offline password guessing against captured material. This sample does not establish that the actual password can be recovered within any practical time.

SECTION AD-06 / CONTINUED

Reproduction, remediation and verification

Root cause

An account-level exception removes a Kerberos protection without an agreed current dependency. Exposure and crackability are different facts.

Reproduction approach

- 1 Confirm the account exception and the authorised protocol endpoint.
- 2 Request only the scoped response and preserve the minimum protocol evidence.
- 3 Apply the agreed offline time/attempt budget; record the negative result honestly.
- 4 Compare with the protected control account and stop without claiming a logon.

Remediation

- Restore pre-authentication after verifying the legacy dependency; remove unused accounts.
- Rotate the service secret and use supported managed identities where appropriate.

Retest acceptance criteria - not performed

The same unauthenticated request now requires pre-authentication, the authorised service works, and the documented exception is removed.

Handoff. A real finding includes the exact principal, timestamps, configuration, response and secure evidence reference. Never paste a recovered password into a broadly distributed report.

SECTION AD-04

A readable deployment script exposes a service identity

Synthetic evidence; no real assessment was executed.

Report severity	MEDIUM
CVSS v3.1 Base	4.3 / Medium (illustrative Base) CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N Ordinary share reader obtains a usable, scoped service identity.
Component	Deployment script on FILE-01 and the scoped svc_lab_backup account.
Starting access	Ordinary user read access to the named lab share; no administrator access.
ATT&CK	T1552.001
Status	Illustrative / NOT RETESTED

Description

A script readable by the ordinary lab group contains a synthetic service password. A minimal authentication probe confirms it is current; an administrative operation is denied. The report records the file path, ownership and validity without publishing the secret or reading backup content.

SYNTHETIC EVIDENCE / NOT A CAPTURED SESSION

```
AD04-E1 | \FILE-01.example.test\LabDeploy\backup.ps1
AD04-E1 | identity: svc_lab_backup | secret: [WITHHELD]
AD04-E2 | minimal authentication probe: accepted
AD04-E3 | administrator-only test: denied
STOP    | no backup archive opened; no password reuse test
```

Illustrated impact and stop point

The exposed service identity is usable within its observed scope. Broader rights, password reuse, backup disclosure and domain privilege remain untested.

SECTION AD-04 / CONTINUED

Reproduction, remediation and verification

Root cause

A reusable secret is distributed through a file whose readers exceed the intended service boundary. File encryption without removing the exposed reusable credential is not sufficient remediation.

Reproduction approach

- 1 Record the permitted share/path and effective read access as the ordinary test user.
- 2 Inspect only the scoped script; redact the credential in the report and preserve secure evidence separately in a real engagement.
- 3 Validate current authentication with a minimal probe; do not retrieve backup contents.
- 4 Record the denied administrative control and stop without testing reuse elsewhere.

Remediation

- Rotate and invalidate the exposed credential; review available access evidence before removing the script.
- Replace stored passwords with a supported managed identity/secret retrieval mechanism and narrow share permissions.

Retest acceptance criteria - not performed

The original file and copies no longer expose the secret; the old secret fails; the intended service still runs under scoped rights.

Handoff. A real finding includes the exact principal, timestamps, configuration, response and secure evidence reference. Never paste a recovered password into a broadly distributed report.

SECTION AD-02

Relayed authentication permits a bounded LDAP read

Synthetic evidence; no real assessment was executed.

Report severity	MEDIUM
CVSS v3.1 Base	3.1 / Low (illustrative Base) CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N Adjacent-network relay; only the bounded directory read succeeded.
Component	DC-01 LDAP signing policy, authentication path and directory permissions.
Starting access	Authorised on-network test host and an agreed lab machine authentication source.
ATT&CK	T1557.001
Status	Illustrative / NOT RETESTED

Description

The lab accepts a relayed NTLM exchange over an LDAP path that does not require signing. The relayed machine identity can read a small agreed set of directory attributes. A controlled write to a protected test object is denied. The result is authenticated read exposure, not automatic Domain Admin or a writable directory.

SYNTHETIC EVIDENCE / NOT A CAPTURED SESSION

```
AD02-E1 | source: WS-LAB$ | target: DC-01.example.test LDAP
AD02-E1 | signing required on tested path: no
AD02-E2 | relayed bind: accepted as EXAMPLE\WS-LAB$
AD02-E2 | agreed test-container read: accepted
AD02-E3 | protected test-object write: denied
CONTROL | anonymous read of the same container: denied
```

Illustrated impact and stop point

The sample shows directory information accessible through relayed authentication. No ACL modification, AD CS enrolment, DCSync or domain takeover is established. Signing requirements on another host are not inferred.

SECTION AD-02 / CONTINUED

Reproduction, remediation and verification

Root cause

The authentication channel accepts a relayable exchange without the required integrity protection. Effective permissions still constrain what the relayed identity can do. LDAP signing and LDAPS channel binding are different controls and must be tested on their actual paths.

Reproduction approach

- 1 Agree the source machine, target service, read attributes and one reversible negative-control operation.
- 2 Record the protocol and signing negotiation before exercising the agreed relay.
- 3 Read only the named lab container through the accepted machine identity.
- 4 Compare anonymous access and protected-object write; preserve the denials and terminate the relay session.

Remediation

- Require LDAP signing on the tested path after compatibility review; apply channel binding where the tested TLS path requires it.
- Reduce NTLM exposure and unnecessary name-resolution/authentication paths; monitor service-specific failures during rollout.

Retest acceptance criteria - not performed

Repeat the same source/target/protocol: the relayed bind must fail while authorised signed clients still work. Verify LDAPS and other endpoints separately.

Handoff. A real finding includes the exact principal, timestamps, configuration, response and secure evidence reference. Never paste a recovered password into a broadly distributed report.

SECTION AD-05

Null-session enumeration discloses lab account names

Synthetic evidence; no real assessment was executed.

Report severity	LOW
CVSS v3.1 Base	5.3 / Medium (illustrative Base) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Limited account-name disclosure; protected file content remained denied.
Component	Anonymous SMB/RPC enumeration policy on FILE-01.
Starting access	On-network access to the named SMB endpoint, without a domain identity.
ATT&CK	T1087.002
Status	Illustrative / NOT RETESTED

Description

An anonymous RPC enumeration returns a small set of synthetic account names from the scoped endpoint. A separate anonymous file-content request is denied. This is information disclosure that lowers reconnaissance effort; account names are not passwords and the result is not anonymous directory administration.

SYNTHETIC EVIDENCE / NOT A CAPTURED SESSION

```
AD05-E1 | endpoint: FILE-01.example.test | identity: anonymous
AD05-E2 | scoped account-name query: alice, bob, svc_lab_backup
AD05-E3 | anonymous LabPrivate file-content request: denied
STOP    | no spraying, brute force or account takeover
```

Illustrated impact and stop point

Limited account-name disclosure supports reconnaissance. No credential validity, user impersonation or sensitive file access is demonstrated.

SECTION AD-05 / CONTINUED

Reproduction, remediation and verification

Root cause

The endpoint permits a directory-information operation to an unauthenticated caller beyond the documented requirement. RootDSE discovery alone would not establish this finding.

Reproduction approach

- 1 Confirm an unauthenticated session and the exact endpoint; do not reuse a cached domain token.
- 2 Run only the agreed account-name enumeration and preserve the minimal synthetic result.
- 3 Verify an anonymous request for protected content is denied.
- 4 End the session without password attacks or user-contact activity.

Remediation

- Restrict the unnecessary anonymous enumeration operation after reviewing legacy compatibility.
- Apply consistent policies to the actual endpoints, not only the domain-controller baseline.

Retest acceptance criteria - not performed

Anonymous account enumeration is denied; authorised inventory tooling continues to work; protected content remains denied.

Handoff. A real finding includes the exact principal, timestamps, configuration, response and secure evidence reference. Never paste a recovered password into a broadly distributed report.

SECTION 05

Remediation sequence

Cut the demonstrated paths before treating the inventory as a checklist.

Wave	Actions	Confirmation
1 / AD-01,03,04	Remove excessive privilege; rotate exposed identities; review service dependencies.	Old identity/path denied; legitimate service preserved.
2 / AD-02,06	Enforce protocol integrity and pre-authentication; verify actual client paths.	Relay/pre-auth controls pass without client regressions.
3 / AD-05	Restrict unnecessary anonymous enumeration and check equivalent endpoints.	Anonymous denial and authorised inventory success.

Owners and dependencies

A real plan assigns each item to an accountable identity/network/application owner and an agreed date. Those business values are not invented here. Coordinate service-account rotation, delegation cleanup and session refresh so that a closed configuration does not leave an old token usable.

SECTION 06

Retest and closure

No fixes were supplied or retested for this fictional lab. All findings remain NOT RETESTED.

ID	Required confirmation	Status
AD-03	The original support user cannot change the privileged membership; an authorised administrator can; the fresh-token sentinel remains denied for the test principal.	NOT RETESTED
AD-01	The service still works with least privilege; the old secret is rejected; ordinary users cannot reach the privileged sentinel. A failed crack alone does not prove all service identities safe.	NOT RETESTED
AD-06	The same unauthenticated request now requires pre-authentication, the authorised service works, and the documented exception is removed.	NOT RETESTED
AD-04	The original file and copies no longer expose the secret; the old secret fails; the intended service still runs under scoped rights.	NOT RETESTED
AD-02	Repeat the same source/target/protocol: the relayed bind must fail while authorised signed clients still work. Verify LDAPS and other endpoints separately.	NOT RETESTED
AD-05	Anonymous account enumeration is denied; authorised inventory tooling continues to work; protected content remains denied.	NOT RETESTED

Closure rules

Closed requires the original attack transition to fail under equivalent starting conditions while the legitimate operation works. Partially resolved records a remaining route or incomplete coverage. Unavailable targets stay unverified. A path can be blocked by one fixed edge while other underlying findings remain open.

SECTION APPENDIX

Evidence, cleanup and references

An explicit boundary is part of a useful report.

Evidence register

N-01: discovery/service inventory; AD01-E1-E4: identity/ticket/recovery/privilege/single-account replication; AD02-E1-E3: protocol/bind/read/denial; AD03-E1-E3: ACL/host mapping/change/restoration; AD04-E1-E3: file/authentication/denial; AD05-E1-E3: anonymous enumeration/protected-content denial; AD06-E1-E3: exception/response/unsuccessful recovery. Every item is synthetic.

Cleanup and real delivery

The illustrated membership change is reversed and verified with a fresh logon. Real delivery also records the deletion of temporary artefacts, terminated relay sessions, securely transferred evidence and client-owned credential rotation. Retest and cleanup are different activities; no production cleanup was performed for this fictional document.

References and assurance limits

CVSS is owned by FIRST and used by permission. Scores and vectors follow CVSS v3.1 Base.

ATT&CK; identifiers classify the illustrated techniques; they do not certify coverage. Tool output does not replace effective-access validation. This is not a compliance opinion, certification or guarantee of a secure domain.

<https://www.first.org/cvss/v3.1/specification-document>

<https://attack.mitre.org/techniques/T1558/003/>

<https://attack.mitre.org/techniques/T1557/001/>

<https://attack.mitre.org/techniques/T1098/007/>

<https://attack.mitre.org/techniques/T1552/001/>

<https://attack.mitre.org/techniques/T1087/002/>

<https://attack.mitre.org/techniques/T1558/004/>

PXLSec / PXLSecurity LTD.

12 Vasil Levski Blvd., 1142 Sofia, Bulgaria

hello@pxlsec.com / pxlsec.com