



INTERNAL NETWORK / ACTIVE DIRECTORY - СИНТЕТИЧЕН ПРИМЕР

Вътрешна мрежа и Active Directory

От началния достъп до границата, която действително издържа.

Измислена лаборатория, не клиентски тест. Всички идентичности, хостове, записи, пътища и резултати са синтетични. За този пример не е тествана production мрежа. Показва резултата от работата и границите на изводите.

6 констатации / 3 примерни пътя
2 High / 3 Medium / 1 Low
Доказателства, контроли, cleanup и retest критерии

PXLSec / PXLSecurity LTD.
29 October 2026 / v1.0

SECTION READ FIRST

Контрол на документа и съдържание

Публичен маркетингов пример. Не представя реален клиент, production тайна или изпълнена атака.

Документ	PXLSec-AD-SAMPLE / v1.0
Класификация	Публичен синтетичен пример; без клиентски данни
Среда	EXAMPLE.TEST / TEST-NET 192.0.2.0/24
Статус на доказателствата	Всеки evidence блок е създаден за илюстрация.
Retest статус	NOT RETESTED

Раздел	Съдържание	Стр.
01	Обобщение	3
02	Обхват и начални позиции	4
03	Метод, покритие и безопасност	5
03A	Ход на теста	6
04	Констатации и технически доказателства	9
05	Последователност на корекциите	22
06	Повторен тест и затваряне	23
APPENDIX	Доказателства, cleanup и източници	24

SECTION 01

Обобщение

Една мрежа може да допуска един privilege път и да отказва друг.

6	9	0
примерни констатации	етапа в разказа	реални клиенти

В измислената лаборатория има две High, три Medium и една Low констатация. Възстановима привилегирована служебна идентичност позволява контролирана демонстрация на домейн credential replication. Прекомерна групова делегация достига един member server. Отделна relay проверка показва само ограничено LDAP четене: защитеният write е отказан.

Главата за хода на теста проследява лабораторното упражнение и всяка промяна на началната идентичност. Тайна във файл, anonymous изброяване и pre-authentication изключение имат независими предпоставки и ограничени резултати. Никоя констатация не е обявена за domain compromise само защото инструмент я е изброил.

Първи решения

- 1 Премахнете ненужните домейн права и group-control делегации при запазени service зависимости.
- 2 Оттеглете изложените идентичности и коригирайте конкретните authentication пътища, включително signing.
- 3 Повторете всеки първоначален път с контролите му; снимка на настройка не е затваряне.

Работещи контроли. Защитен LDAP write, anonymous file read и достъп с обновен token след cleanup са отказани в примера. Тези граници са част от резултата.

SECTION 02

Обхват и начални позиции

Всеки път е свързан със собствен акаунт, хост и разрешено действие.

Домейн	EXAMPLE.TEST (fictional)
Цели	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
Начални идентичности	Anonymous on-network host; обикновен alice; делегиран support user; собствен test principal.
Разрешение	Реален тест изисква подписан списък с цели и правила. За този пример не е изпълняван тест.
Исключено	Cloud identity, trusts, AD CS exploitation, OT, phishing, password spraying, масова credential replication, разрушителни тестове и несвързани хостове.

Оперативни контроли

- Уговорете source адреси, credentials, прозорци, контакт за ескалация и stop условия преди активни проверки.
- Използвайте собствени test objects и обратими членства; не предизвиквайте удостоверяване от реални потребители извън изричния обхват.
- Исключеното е непроверено, не сигурно. Разрешен прочит на един container не разрешава full directory dump.

SECTION 03

Метод, покритие и безопасност

Открийте връзката, проверете прехода и запишете както успеха, така и отказа.

Област	Покритие в примера	Граница
Kerberos	AD-01, AD-06	Една възстановена lab тайна; един неуспех.
LDAP / NTLM	AD-02	Bind/read приети, protected write отказан.
Delegation / ACL	AD-03	Един обратим group-to-host път.
Shares / secrets	AD-04, AD-05	Само scoped script и account имена.
AD CS / trusts / cloud	Не е изпълнявано	Без извод за сигурност.

Доказателства и severity

Всеки evidence ID обозначава наблюдение и principal. Графична връзка сама по себе си не проверява път. Severity зависи от описания lab достъп и операция. Примерните CVSS v3.1 Base оценки са изчислени от пълните вектори във всяка констатация. Severity в доклада е контекстен приоритет и може да се различава от CVSS Base категорията.

Детекция и безопасност

Реалният handoff съпоставя ticket, bind, logon и group-change доказателствата с наличната defender telemetry. Примерът не измисля SIEM alerts, EDR evasion или времена за детекция. Availability и lockout ограниченията имат предимство пред по-дълъг път.

SECTION 03A

Ход на теста

Откриване, проверка, експлоатация и следваща стъпка.

Примерна възстановка. Разказът описва констатациите в хронологичен ред, а не новоизпълнен клиентски тест. Предоставеният достъп и отделните проверки са посочени изрично.

01 / Сканирахме уговорения вътрешен диапазон

Започнахме от разрешения тестов хост във вътрешната мрежа с откриване на системи и сканиране на услугите в обхват. Идентифицирахме DC-01, FILE-01, SQL-01 и APP-01 и услугите SMB, LDAP и Kerberos. Съпоставихме отговорите с DNS и уговорените цели. За удостоверената фаза имахме предоставен обикновен акаунт alice; сканирането не ни го осигури.

Доказателства: N-01: synthetic discovery/service inventory; scope

02 / Anonymous изброяването разкри имена на акаунти

Преди да използваме alice, проверихме неудоверения SMB/RPC достъп до FILE-01. Заявката за акаунти върна alice, bob и svc_lab_backup. Anonymous достъпът до защитени файлове беше отказан. Записахме разкриването на имена и преминахме изрично към предоставения акаунт за преглед на shares, без password spraying или измислено превземане на акаунт.

Доказателства: AD-05 / AD05-E1-E3

03 / В deployment share намерихме работещ credential

Като alice изброихме четимите shares и прегледахме уговорения script в LabDeploy на FILE-01. В него имаше синтетична парола за svc_lab_backup. Удостоверихме се с акаунта и потвърдихме валидността; административна операция беше отказана. Имахме използвана служебна идентичност, но още не Domain Admin. Не отваряхме backup архиви и не проверявахме reuse върху други системи.

Доказателства: AD-04 / AD04-E1-E3

SECTION 03A / 2

Ход на теста

Откриване, проверка, експлоатация и следваща стъпка.

04 / Domain enumeration разкри следващата възможност за повишаване на права

С удостоверения домейн достъп разгледахме service principals, членства и делегации. svc_lab_sql имаше MSSQLSvc SPN и ненужно Domain Admin членство. Комбинацията направи билета му ценна офлайн цел. Поискахме само разрешения билет и записахме идентичността и правата, които биха били достъпни при успешно възстановяване на паролата.

Доказателства: AD-01 / AD01-E1

05 / Kerberoasting възстанови привилегированата lab парола

Проверихме получения service ticket в уговорения офлайн бюджет. Успяхме да възстановим служебната парола. Удостоверихме се като svc_lab_sql и потвърдихме домейн правата с уговорената контролна операция; същата операция като alice беше отказана. Повишаването на права зависи и от възстановяването, и от прекомерното членство, а не само от наличен SPN.

Доказателства: AD-01 / AD01-E2-E3

06 / Демонстрирахме достъп до домейн credential hash в лабораторията

За да потвърдим въздействието върху домейн credentials, продължихме с изрично разрешена replication проверка към DC-01. С възстановената привилегирована идентичност поискахме данни само за един специален сапary акаунт. Отговорът съдържаеше неговия NT hash и показва въздействието върху домейн credentials. Хашът е скрит в публичния пример. Не извличахме всички домейн хашове, krbtgt материал и не използвахме сапary хаша за следващ вход.

Доказателства: AD-01 / AD01-E4: synthetic single-account replication

SECTION 03A / 3

Ход на теста

Откриване, проверка, експлоатация и следваща стъпка.

07 / Продължихме с делегациите и достъпа до сървър

След домейн ескалацията се върнахме към отделно предоставената support-user позиция, за да не прикрием по-слаби контроли с Domain Admin права. Делегацията позволяваше промяна на LAB-App-Admins, свързана с local administration на APP-01. Направихме обратима промяна на членството, създадохме нова сесия и потвърдихме административна sentinel операция. После върнахме членството и проверихме отказ с обновена сесия.

Доказателства: AD-03 / AD03-E1-E3

08 / Relay и AS-REP проверките дадоха различни резултати

След това изпълнихме отделно уговорената machine-authentication relay проверка. LDAP прие идентичността и разреши ограничено четене, но отказа защитения запис. Накрая акаунт с изключена pre-authentication върна AS-REP материал; ограниченото възстановяване беше неуспешно. Нито една проверка не осигури предишния Domain Admin достъп. Описахме и успеха, и неуспешните продължения.

Доказателства: AD-02 / AD02-E1-E3; AD-06 / AD06-E1-E3

09 / Приключихме упражнението и подготвихме доказателствата

Прекратихме сесиите, потвърдихме върнатото членство и описахме засегнатите идентичности за ротация от клиента. Регистърът свързва откриването, exposed credentials, възстановяването от service ticket, единичната replication проверка и server достъпа с констатациите. Не добавяхме persistence и не представяме корекции като повторно проверени. Цялата хронология е преработен измислен lab сценарий.

Доказателства: Evidence register; cleanup; retest status

SECTION 04

Констатации и технически доказателства

Шест независими констатации. Всеки evidence блок по-долу е синтетичен.

ID	Констатация	Severity	CVSS 3.1
AD-03	Делегирана промяна на група достига един member server	High	8.8
AD-01	Възстановима служебна парола предоставя домейн привилегии	High	7.5
AD-06	Lab акаунт е с изключена Kerberos pre-authentication	Medium	5.3
AD-04	Четим deployment script разкрива служебна идентичност	Medium	4.3
AD-02	Препредадено удостоверяване позволява ограничено LDAP четене	Medium	3.1
AD-05	Null-session изброяване разкрива lab account имена	Low	5.3

Всички finding статуси са Илюстративно / NOT RETESTED. Синтетичен успех не доказва компрометиране на реална организация.

SECTION AD-03

Делегирана промяна на група достига един member server

Синтетични доказателства; не е изпълняван реален тест.

Критичност в доклада	HIGH
CVSS v3.1 Base	8.8 / High (примерна Base оценка) CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H Съществуващ делегиран user; административни права върху един member server.
Компонент	ACL на LAB-App-Admins и local-administrator назначението на APP-01.
Начален достъп	Обикновен user с наследена support делегация; една разрешена обратима промяна на група.
ATT&CK	T1098.007
Статус	Illustrative / NOT RETESTED

Описание

Support група може да променя LAB-App-Admins, която е local Administrators на един lab application server. Добавя се само специален test principal, създава се нов logon и се проверява безвреден administrator-only sentinel. Премахване на членството и нов token връщат отказа.

СИНТЕТИЧНИ ДОКАЗАТЕЛСТВА / НЕ Е ЗАСНЕТА СЕСИЯ

```
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
```

Примерно въздействие и точка на спиране

Илюстрирани са административни права на APP-01. Не са установени DC administration, достъп до други сървъри или persistence. При remediation се отчитат кешираните tokens.

SECTION AD-03 / CONTINUED

Възпроизвеждане, корекции и проверка

Първопричина

Делегирано административно право пресича непредвидена privilege граница. Членства, вложени групи и ефективни локални права се оценяват заедно.

Подход за възпроизвеждане

- 1 Запишете началния user, наследения ACL и group-to-host назначението.
- 2 Потвърдете, че test principal няма достъп до уговорената административна операция.
- 3 Приложете уговорената промяна, получите нов token и изпълнете само безвредния sentinel.
- 4 Премахнете членството, проверете възстановеното състояние и повторете с нов login.

Корекции

- Премахнете ненужната делегация за членство и прегледайте наследените/вложени пътища.
- Ограничете управлението на privileged групи и обновете/оттеглете засегнатите сесии по плана за реакция.

Критерии за retest - не е изпълняван

Първоначалният support user не може да променя privileged членството, легитимният администратор може, а sentinel с нов token остава отказан за test principal.

Handoff. Реална констатация включва точен principal, timestamps, конфигурация, отговор и защитен evidence reference. Не публикувайте възстановена парола в широко разпространяван доклад.

SECTION AD-01

Възстановима служебна парола предоставя домейн привилегии

Синтетични доказателства; не е изпълняван реален тест.

Критичност в доклада	HIGH
CVSS v3.1 Base	7.5 / High (примерна Base оценка) CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H Нужно е офлайн възстановяване; намерената идентичност има домейн права.
Компонент	svc_lab_sql, неговият SPN, паролата и членството в привилегирована група.
Начален достъп	Обикновен EXAMPLE.TEST user; достъп до Kerberos и разрешения lab билет.
ATT&CK	T1558.003
Статус	Illustrative / NOT RETESTED

Описание

Измисленият service account съчетава SPN, умишлено възстановима lab парола и Domain Admin членство. Обикновен акаунт може да поиска билета. Ограничена офлайн проверка възстановява lab тайната, а проверка потвърждава правата. Отделно разрешена replication проверка показва достъп до NT hash на един canary акаунт. Наличен билет, успешното възстановяване и ефективните права са отделни наблюдения.

СИНТЕТИЧНИ ДОКАЗАТЕЛСТВА / НЕ Е ЗАСНЕТА СЕСИЯ

```
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
```

Примерно въздействие и точка на спиране

За тази lab идентичност са илюстрирани домейн права. Възстановяването зависи от действителната тайна и тестовия бюджет. Отделно разрешена replication проверка върна NT hash на един измислен canary акаунт (AD01-E4), със скрита стойност. Няма масово извличане, krbtgt, използване на хаша или persistence.

SECTION AD-01 / CONTINUED

Възпроизвеждане, корекции и проверка

Първопричина

Служебна идентичност има ненужни домейн права и парола, която не покрива уговорената устойчивост. Самият SPN е нормален и не е констатацията.

Подход за възпроизвеждане

- 1 Потвърдете test user, разрешения service principal и ефективното членство.
- 2 Съберете само уговорения билет; запишете акаунта и обхвата.
- 3 Изпълнете ограничената офлайн проверка; не включвайте тайната в разпространявания PDF.
- 4 Удостоверете lab идентичността, сравнете privileged проверката с обикновения user и изпълнете само отделно разрешената single-canary replication проверка.

Корекции

- Премахнете ненужното Domain Admin членство след проверка на зависимостите.
- Използвайте поддържана managed service identity или силна случайна парола с ротация; оттеглете изложената тайна.

Критерии за retest - не е изпълняван

Услугата работи с минимални права, старата тайна е отказана, а обикновените users не достигат privileged sentinel. Неуспешно cracking само по себе си не доказва сигурността на всички идентичности.

Handoff. Реална констатация включва точен principal, timestamps, конфигурация, отговор и защитен evidence reference. Не публикувайте възстановена парола в широко разпространяван доклад.

SECTION AD-06

Lab акаунт е с изключена Kerberos pre-authentication

Синтетични доказателства; не е изпълняван реален тест.

Критичност в доклада	MEDIUM
CVSS v3.1 Base	5.3 / Medium (примерна Base оценка) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Изложен pre-authentication отговор; няма възстановена парола или вход.
Компонент	Pre-authentication настройката на svc_lab_legacy.
Начален достъп	Известен scoped lab акаунт и достъп до Kerberos endpoint на домейна.
ATT&CK	T1558.004
Статус	Illustrative / NOT RETESTED

Описание

Scoped акаунтът връща roastable AS response без pre-authentication. Ограниченият офлайн тест не възстановява паролата. Това е control weakness, но изрично не се заявяват възстановена парола, удостоверен foothold или привилегировано продължение.

СИНТЕТИЧНИ ДОКАЗАТЕЛСТВА / НЕ Е ЗАСЧЕТА СЕСИЯ

```
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
```

Примерно въздействие и точка на спиране

Акаунтът позволява офлайн guessing върху получения материал. Примерът не установява практически възстановяване на действителната парола.

SECTION AD-06 / CONTINUED

Възпроизвеждане, корекции и проверка

Първопричина

Account-level изключение премахва Kerberos защита без уговорена текуща зависимост. Exposure и crackability са различни факти.

Подход за възпроизвеждане

- 1 Потвърдете account изключението и разрешения protocol endpoint.
- 2 Поискайте само scoped response и пазете минималните protocol доказателства.
- 3 Приложете уговорения офлайн бюджет; запишете отрицателния резултат.
- 4 Сравнете със защитения контролен акаунт и спрете без твърдение за login.

Корекции

- Възстановете pre-authentication след проверка на legacy зависимостта; премахнете неизползваните акаунти.
- Ротирайте служебната тайна и използвайте поддържани managed identities, когато е приложимо.

Критерии за retest - не е изпълняван

Същата неустоверена заявка изисква pre-authentication, услугата работи, а изключението е премахнато.

Handoff. Реална констатация включва точен principal, timestamps, конфигурация, отговор и защитен evidence reference. Не публикувайте възстановена парола в широко разпространяван доклад.

SECTION AD-04

Четим deployment script разкрива служебна идентичност

Синтетични доказателства; не е изпълняван реален тест.

Критичност в доклада	MEDIUM
CVSS v3.1 Base	4.3 / Medium (примерна Base оценка) CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N Читател на share получава използваема служебна идентичност с ограничени права.
Компонент	Deployment script на FILE-01 и ограниченият svc_lab_backup акаунт.
Начален достъп	Read достъп на обикновен user до посочения lab share; без административни права.
ATT&CK	T1552.001
Статус	Illustrative / NOT RETESTED

Описание

Script, четим от обикновената lab група, съдържа синтетична служебна парола. Минимално удостоверяване потвърждава валидността, а административна операция е отказана. Записани са пътят, собственикът и валидността, без тайната или backup съдържание.

СИНТЕТИЧНИ ДОКАЗАТЕЛСТВА / НЕ Е ЗАЧЕТА СЕСИЯ

```
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
```

Примерно въздействие и точка на спиране

Изложената идентичност е използваема в наблюдавания обхват. По-широки права, reuse, backup disclosure и домейн привилегии остават непроверени.

SECTION AD-04 / CONTINUED

Възпроизвеждане, корекции и проверка

Първопричина

Повторно използвана тайна се разпространява чрез файл с прекалено широки читатели. Криптиране на файла без оттегляне на тайната не е достатъчна корекция.

Подход за възпроизвеждане

- 1 Запишете разрешения share/path и ефективния read достъп с обикновения test user.
- 2 Прегледайте само scoped script; редактирайте credential-a в доклада и пазете реалните доказателства отделно по защитен канал.
- 3 Проверете текущото удостоверяване с минимална заявка, без backup съдържание.
- 4 Запишете отказаната административна контрола и спрете без reuse тестове другаде.

Корекции

- Ротирайте и обезсилете credential-a; прегледайте наличните access доказателства преди премахване на script-a.
- Заменете записаните пароли с поддържана managed identity/secret retrieval схема и ограничете share правата.

Критерии за retest - не е изпълняван

Първоначалният файл и копията не разкриват тайната, старата парола е отказана, а услугата работи с ограничени права.

Handoff. Реална констатация включва точен principal, timestamps, конфигурация, отговор и защитен evidence reference. Не публикувайте възстановена парола в широко разпространяван доклад.

SECTION AD-02

Препредадено удостоверяване позволява ограничено LDAP четене

Синтетични доказателства; не е изпълняван реален тест.

Критичност в доклада	MEDIUM
CVSS v3.1 Base	3.1 / Low (примерна Base оценка) CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N Relay от съседна мрежа; успешен е само ограниченият directory прочит.
Компонент	LDAP signing политиката на DC-01, пътят за удостоверяване и directory правата.
Начален достъп	Разрешен on-network test host и уговорен източник на lab machine удостоверяване.
ATT&CK	T1557.001
Статус	Illustrative / NOT RETESTED

Описание

Лабораторията приема препредаден NTLM обмен през LDAP път без задължително signing. Machine идентичността чете малък уговорен набор от directory атрибути. Контролиран write към защитен test object е отказан. Резултатът е read exposure, не автоматичен Domain Admin или writable directory.

СИНТЕТИЧНИ ДОКАЗАТЕЛСТВА / НЕ Е ЗАЧЕТА СЕСИЯ

```
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
```

Примерно въздействие и точка на спиране

Примерът показва directory информация през relay. Не са установени ACL промяна, AD CS enrolment, DCSync или domain takeover. Не се правят изводи за signing на други хостове.

SECTION AD-02 / CONTINUED

Възпроизвеждане, корекции и проверка

Първопричина

Каналът приема relayable обмен без нужната integrity защита. Ефективните права продължават да ограничават идентичността. LDAP signing и LDAPS channel binding са различни контроли и се проверяват по съответните пътища.

Подход за възпроизвеждане

- 1 Уговорете source machine, target service, read атрибутите и една обратима отрицателна проверка.
- 2 Запишете протокола и signing negotiation преди уговорената relay проверка.
- 3 Прочетете само посочения lab container с приетата machine идентичност.
- 4 Сравнете anonymous достъп и write към защитения обект; запазете отказите и прекратете сесията.

Корекции

- Изисквайте LDAP signing по тествания път след compatibility review; приложете channel binding за съответния TLS път.
- Намалете NTLM exposure и ненужните name-resolution/authentication пътища; следете service-specific грешките при внедряване.

Критерии за retest - не е изпълняван

Повторете същите source/target/protocol: relay bind трябва да е отказан, а легитимните подписани клиенти да работят. LDAPS и другите endpoints се проверяват отделно.

Handoff. Реална констатация включва точен principal, timestamps, конфигурация, отговор и защитен evidence reference. Не публикувайте възстановена парола в широко разпространяван доклад.

SECTION AD-05

Null-session изброяване разкрива lab account имена

Синтетични доказателства; не е изпълняван реален тест.

Критичност в доклада	LOW
CVSS v3.1 Base	5.3 / Medium (примерна Base оценка) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Ограничено разкриване на имена; защитените файлове остават недостъпни.
Компонент	Anonymous SMB/RPC enumeration политиката на FILE-01.
Начален достъп	On-network достъп до посочения SMB endpoint без домейн идентичност.
ATT&CK	T1087.002
Статус	Illustrative / NOT RETESTED

Описание

Anonymous RPC изброяване връща малък набор синтетични account имена от scoped endpoint. Отделна anonymous заявка за файлово съдържание е отказана. Това улеснява разузнаването, но имената не са пароли и резултатът не е anonymous directory administration.

СИНТЕТИЧНИ ДОКАЗАТЕЛСТВА / НЕ Е ЗАЧЕТА СЕСИЯ

```
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
```

Примерно въздействие и точка на спиране

Ограниченото разкриване на имена подпомага разузнаването. Не са показани валидни credentials, impersonation или чувствителни файлове.

SECTION AD-05 / CONTINUED

Възпроизвеждане, корекции и проверка

Първопричина

Endpoint позволява directory-information операция на неустоверен caller отвъд документираното изискване. Само RootDSE discovery не би доказало тази констатация.

Подход за възпроизвеждане

- 1 Потвърдете unauthenticated сесия и точния endpoint; не използвайте кеширан domain token.
- 2 Изпълнете само уговореното account-name изброяване и пазете минималния резултат.
- 3 Потвърдете отказ за anonymous заявка към защитено съдържание.
- 4 Прекратете сесията без password атаки или контакт с потребители.

Корекции

- Ограничете ненужното anonymous изброяване след проверка на legacy съвместимостта.
- Приложете последователни политики към действителните endpoints, не само към DC baseline.

Критерии за retest - не е изпълняван

Anonymous account изброяването е отказано, легитимният inventory tooling работи, а защитеното съдържание остава недостъпно.

Handoff. Реална констатация включва точен principal, timestamps, конфигурация, отговор и защитен evidence reference. Не публикувайте възстановена парола в широко разпространяван доклад.

SECTION 05

Последователност на корекциите

Прекъснете показаните пътища, преди да третирате inventory като checklist.

Етап	Действия	Потвърждение
1 / AD-01,03,04	Премахнете излишните права, ротирайте изложените идентичности и проверете зависимостите.	Старият път е отказан; услугата работи.
2 / AD-02,06	Наложете protocol integrity и pre-authentication по реалните клиентски пътища.	Контролите работят без client regressions.
3 / AD-05	Ограничете anonymous изброяването и проверете сродните endpoints.	Anonymous отказ и успешен легитимен inventory.

Отговорници и зависимости

Реален план посочва identity/network/application отговорник и уговорена дата. Не ги измисляме в примера. Координирайте ротацията, делегациите и session refresh, така че поправена конфигурация да не оставя използваем стар token.

SECTION 06

Повторен тест и затваряне

За измислената лаборатория няма предоставени или проверени корекции.
Всички findings остават NOT RETESTED.

ID	Нужно потвърждение	Status
AD-03	Първоначалният support user не може да променя privileged членството, легитимният администратор може, а sentinel с нов token остава отказан за test principal.	NOT RETESTED
AD-01	Услугата работи с минимални права, старата тайна е отказана, а обикновените users не достигат privileged sentinel. Неуспешно cracking само по себе си не доказва сигурността на всички идентичности.	NOT RETESTED
AD-06	Същата неудоверена заявка изисква pre-authentication, услугата работи, а изключението е премахнато.	NOT RETESTED
AD-04	Първоначалният файл и копията не разкриват тайната, старата парола е отказана, а услугата работи с ограничени права.	NOT RETESTED
AD-02	Повторете същите source/target/protocol: relay bind трябва да е отказан, а легитимните подписани клиенти да работят. LDAPS и другите endpoints се проверяват отделно.	NOT RETESTED
AD-05	Anonymous account изброяването е отказано, легитимният inventory tooling работи, а защитеното съдържание остава недостъпно.	NOT RETESTED

Правила за затваряне

Closed изисква първоначалният преход да е отказан при съпоставими начални условия, а легитимната операция да работи. Partially resolved означава останал път или непълно покритие. Недостъпните цели остават непроверени. Поправена връзка може да прекъсне път, докато други underlying findings остават отворени.

SECTION APPENDIX

Доказателства, cleanup и източници

Ясната граница е част от полезния доклад.

Регистър на доказателствата

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. Всичко е синтетично.

Cleanup и реално предаване

Примерната промяна на членство е върната и проверена с нов login. Реалното предаване записва и временните artefacts, прекратените relay сесии, защитеното предаване и клиентската ротация. Retest и cleanup са различни дейности; за този измислен документ не е изпълняван production cleanup.

Източници и граници на увереността

CVSS е собственост на FIRST и се използва с разрешение. Оценките и векторите следват CVSS v3.1 Base.

ATT&CK; identifiers класифицират техниките, не сертифицират покритие. Tool output не заменя effective-access проверка. Това не е compliance мнение, сертификация или гаранция за сигурен домейн.

<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