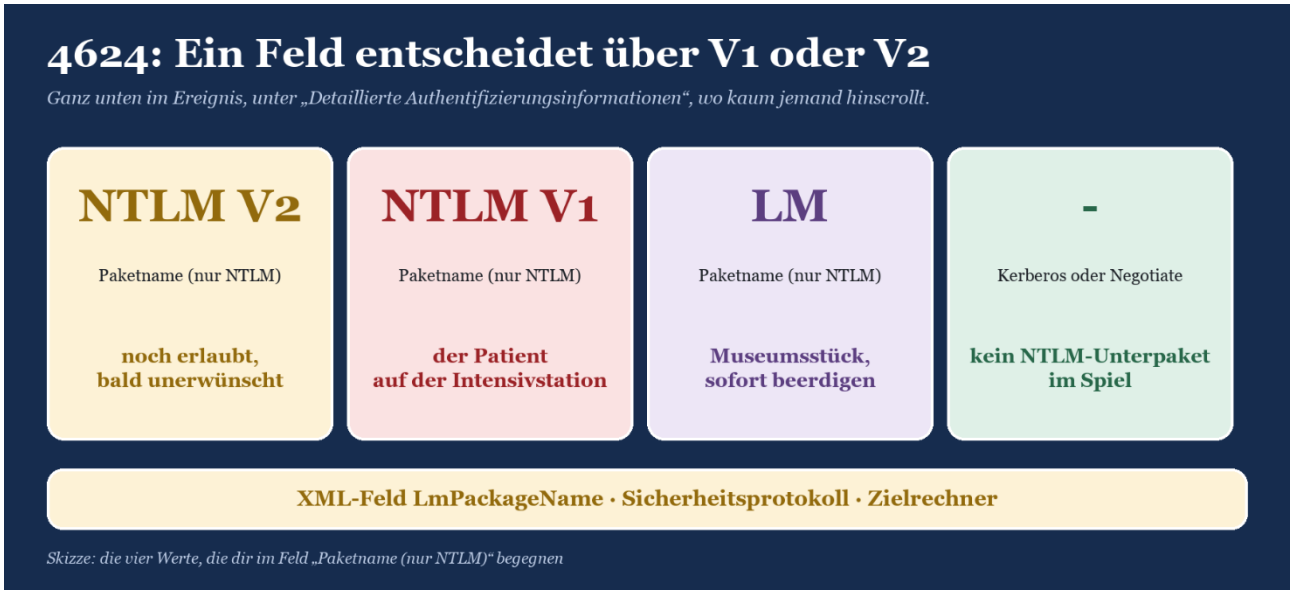
Ereignis 4624: NTLM V1 und V2 im Anmeldeprotokoll erkennen



WISSEN
Was der NTLM Diagnostiker erfasst, wie er arbeitet und was er dir zeigt.
› NTLM Diagnostiker

BERATUNG
NTLMv1 gefunden und keine Ahnung, wer es schickt? Wir suchen mit.
› Beratung zur NTLM-Ablösung

SCHULUNG
Anmeldeprotokoll und NTLM-Ereignisse lesen lernen: für dein ganzes Team.
› Schulung zum NTLM Diagnostiker

Ereignis 4624 ist der Pförtner, der wirklich jeden aufschreibt: den Chef, den Paketboten, die Katze des Hausmeisters und das Dienstkonto, das seit 2014 alle fünf Minuten vorbeischaut, weil niemand mehr weiß, wofür es da ist. Irgendwo in diesem Gästebuch stehen auch die Besucher mit dem verdächtig alten Ausweis. Sie tragen das Kennzeichen „NTLM V1“, und sie stehen ganz unten im Ereignis, im Feld „Paketname (nur NTLM)“, wo kaum jemand hinschaut.

Genau dort solltest du jetzt hinschauen. Seit dem Windows-Update vom 13.10.2026 blockieren Windows 11 ab 24H2 und Windows Server 2025 Single Sign-on mit NTLMv1 standardmäßig; gesteuert wird das über den Registrierungswert BlockNtlmv1SSO, protokolliert über die Ereignisse 4024 und 4025. Mit der nächsten Windows-Server-Version ist NTLM insgesamt ab Werk abgeschaltet. Wer heute noch NTLMv1 im Netz hat, hat also ein Gerät oder eine Anwendung, die entweder schon gerade Ärger macht oder demnächst Ärger machen wird. Die Frage „4624 ntlm v1: wo und wer?“ ist deshalb keine akademische.

In diesem Beitrag liest du 4624 gezielt auf NTLM: welche Felder zählen, wie du V1 und V2 auseinanderhältst, was die Anmeldetypen 3 und 10 bedeuten, wie ein XPath-Filter für die Ereignisanzeige aussieht und wie du mit Get-WinEvent eine erste Hitliste baust. Danach kommt die unbequeme Wahrheit, warum das Sicherheitsprotokoll für eine domänenweite Auswertung viel zu laut ist. Den großen Rahmen der Bestandsaufnahme findest du in NTLM-Nutzung ermitteln, den Zeitplan in Der Fahrplan zur NTLM-Abschaltung.

FAKTEN · Ereignis 4624 in 30 Sekunden

Titel: „Ein Konto wurde erfolgreich angemeldet.“ (englisch „An account was successfully logged on.“), Unterkategorie „Anmelden überwachen“ (Audit Logon), nur Erfolg.

Entsteht auf dem Rechner, an dem die Anmeldung stattfindet, also auf dem Ziel: Dateiserver, Terminalserver, Anwendungsserver, Domain Controller.

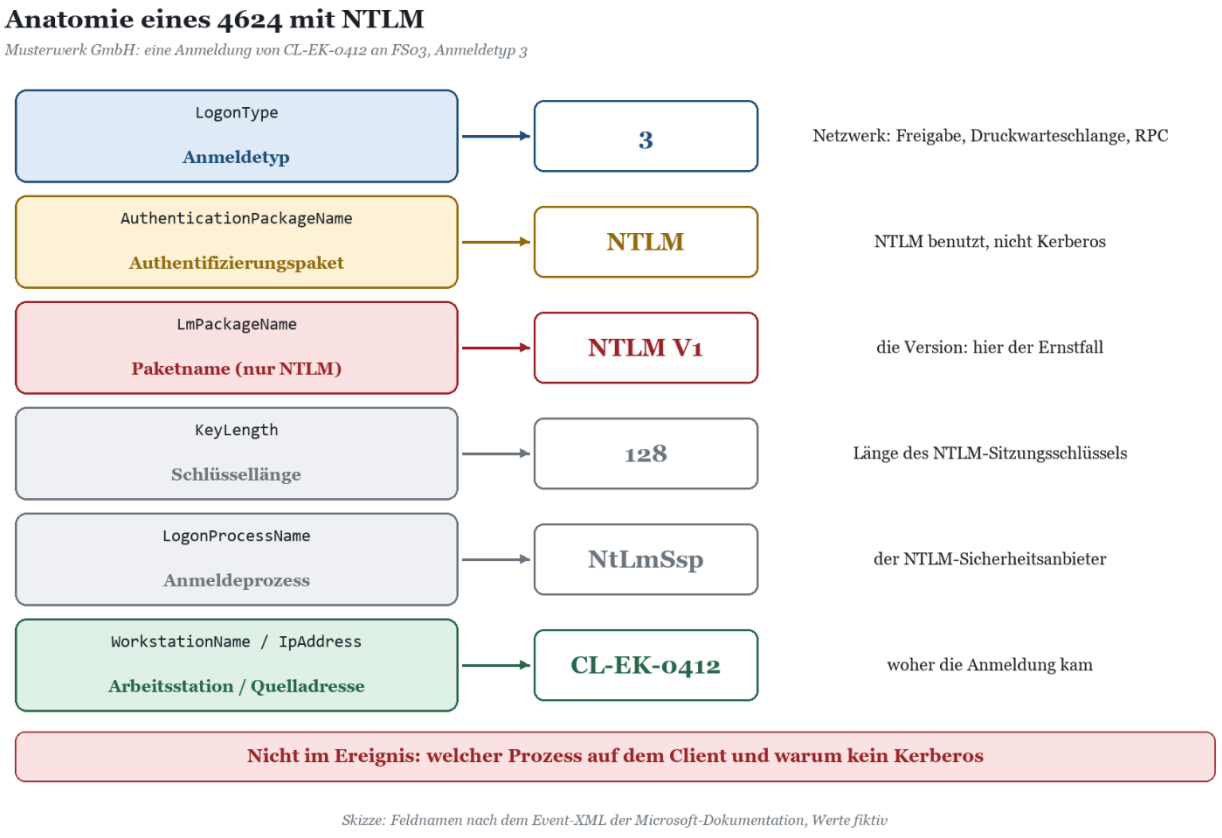
NTLM-relevante XML-Felder: AuthenticationPackageName, LmPackageName, KeyLength, LogonProcessName, LogonType, WorkstationName, IpAddress, TargetUserName.

Mögliche Werte im Paketnamen laut Microsoft: „NTLM V1“, „NTLM V2“ und „LM“; befüllt nur, wenn das Authentifizierungspaket NTLM ist, sonst steht dort ein Bindestrich.

Fehlgeschlagene Anmeldungen landen nicht in 4624, sondern in 4625.

Die NTLM-Felder in 4624: wo V1 und V2 stehen

Öffnest du ein 4624 in der Ereignisanzeige, scrollst du zuerst durch Antragsteller, Anmeldeinformationen, Identitätswechselebene, neue Anmeldung, Prozessinformationen und Netzwerkinformationen. Ganz am Ende kommt der Abschnitt „Detaillierte Authentifizierungsinformationen“. Dort entscheidet sich, ob dich das Ereignis überhaupt interessiert.



Skizze: Feldnamen nach dem Event-XML der Microsoft-Dokumentation, Werte fiktiv

Authentifizierungspaket: NTLM, Kerberos oder Negotiate

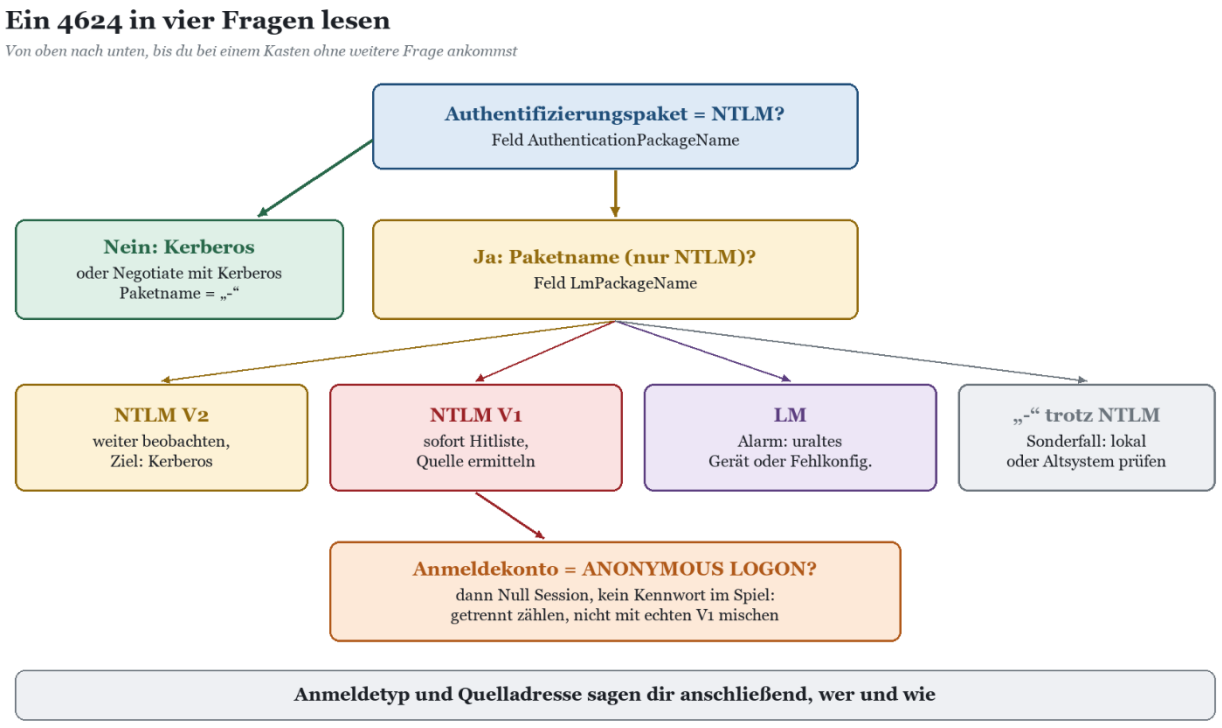
Das Feld „Authentifizierungspaket“ (XML: AuthenticationPackageName) nennt das Paket, das die Anmeldung tatsächlich verarbeitet hat. Für die NTLM-Suche sind drei Werte wichtig: „NTLM“ heißt, dass ein Protokoll der NTLM-Familie benutzt wurde. „Kerberos“ ist das, was du sehen willst. „Negotiate“ bedeutet, dass das Aushandlungspaket gewählt hat; laut Microsoft nimmt es Kerberos, sofern das nicht an einer der Seiten scheitert oder die Anwendung zu wenig Angaben liefert. Steht bei Negotiate die Schlüssellänge auf 0 und der Paketname auf „-“, war es Kerberos.

Daneben siehst du das Feld „Anmeldeprozess“ (LogonProcessName). Bei NTLM-Netzwerkanmeldungen steht dort typischerweise NtLmSsp, bei Kerberos „Kerberos“. Für Filter ist das ein nützliches Zweitmerkmal, maßgeblich bleibt aber das Authentifizierungspaket.

Paketname (nur NTLM): das eigentliche Versionsfeld

Das Feld „Paketname (nur NTLM)“ heißt im XML LmPackageName und nennt das LAN-Manager-Unterpaket, also die Version der NTLM-Familie. Microsoft dokumentiert drei mögliche Werte: „NTLM V1“, „NTLM V2“ und „LM“. Befüllt wird es nur, wenn das Authentifizierungspaket NTLM ist. Steht dort ein Bindestrich, war kein NTLM-Unterpaket beteiligt. Wichtig: Der Wert sagt dir, mit welcher Antwortversion sich der Client am Ziel angemeldet hat. Er sagt nichts darüber, welche Version der Client hätte benutzen können. Ein Client, der V2 kann, aber per LmCompatibilityLevel auf V1 heruntergedreht wurde, sieht im Protokoll genauso aus wie ein Gerät aus dem Jahr 2003.

Paketname (nur NTLM)	Bedeutung	Was du tust
NTLM V2	Anmeldung mit NTLMv2-Antwort	Inventarisieren, mittelfristig auf Kerberos umstellen
NTLM V1	Anmeldung mit NTLMv1-Antwort, kryptografisch schwach	Sofort auf die Hitliste, Quelle ermitteln, abstellen
LM	LAN-Manager-Antwort, noch älter als V1	Alarm: Gerät oder Richtlinie gehört umgehend geprüft
-	kein NTLM-Unterpaket (Kerberos, Negotiate mit Kerberos)	Nichts, das ist der Zielzustand



Skizze: vereinfacht; die Werte stehen so im Event-XML, die Anzeige ist lokalisiert

Schlüssellänge: das unterschätzte Nebenfeld

Die „Schlüssellänge“ (KeyLength) gibt die Länge des NTLM-Sitzungsschlüssels an, üblicherweise 128 oder 56 Bit. Bei Kerberos ist der Wert immer 0. Microsoft empfiehlt ausdrücklich, bei NTLM-Anmeldungen auf eine Schlüssellänge ungleich 128 zu achten, weil alle Windows-Versionen seit Windows 2000 128 Bit beherrschen. Eine 56 neben einem „NTLM V1“ ist also doppelt verdächtig. Eine 0 neben „NTLM V1“ siehst du dagegen häufig bei anonymen Anmeldungen, und damit sind wir beim größten Stolperstein.

WARNUNG · ANONYMOUS LOGON mit NTLM V1 ist ein eigenes Thema

Viele 4624 mit „NTLM V1“ gehören zum Konto ANONYMOUS LOGON (SID S-1-5-7), oft mit Schlüssellänge 0. Das sind Null Sessions: Verbindungen ohne Kennwort, bei denen keine Anmeldeinformationen geprüft werden. Sie sind trotzdem eine Altlast, aber eine andere als ein Benutzer, dessen Kennwort per NTLMv1 übertragen wird.

Zähle beide Gruppen getrennt. Sonst meldest du der IT-Leitung 3.000 NTLMv1-Anmeldungen, und 2.700 davon sind ein Inventarscanner, der anonym Freigaben aufzählt. Wie du diese Fälle aufräumst, liest du hier:

› Anonyme Anmeldungen und Null Sessions: NTLM-Altlasten aufräumen

Wer, woher, wie: die übrigen Felder

Damit aus einem Treffer eine Spur wird, brauchst du noch das angemeldete Konto (TargetUserName und TargetDomainName), den Arbeitsstationsnamen (WorkstationName) und die Quellnetzwerkadresse (IpAddress). Microsoft weist darauf hin, dass diese Netzwerkfelder je nach Protokoll und Dienst unterschiedlich befüllt werden. In der Praxis ist bei NTLM-Netzwerkanmeldungen über SMB meist beides da, bei anderen Diensten fehlt mal die Adresse, mal der Name. Der Arbeitsstationsname stammt außerdem vom Client selbst und ist deshalb ein Hinweis, kein Beweis.

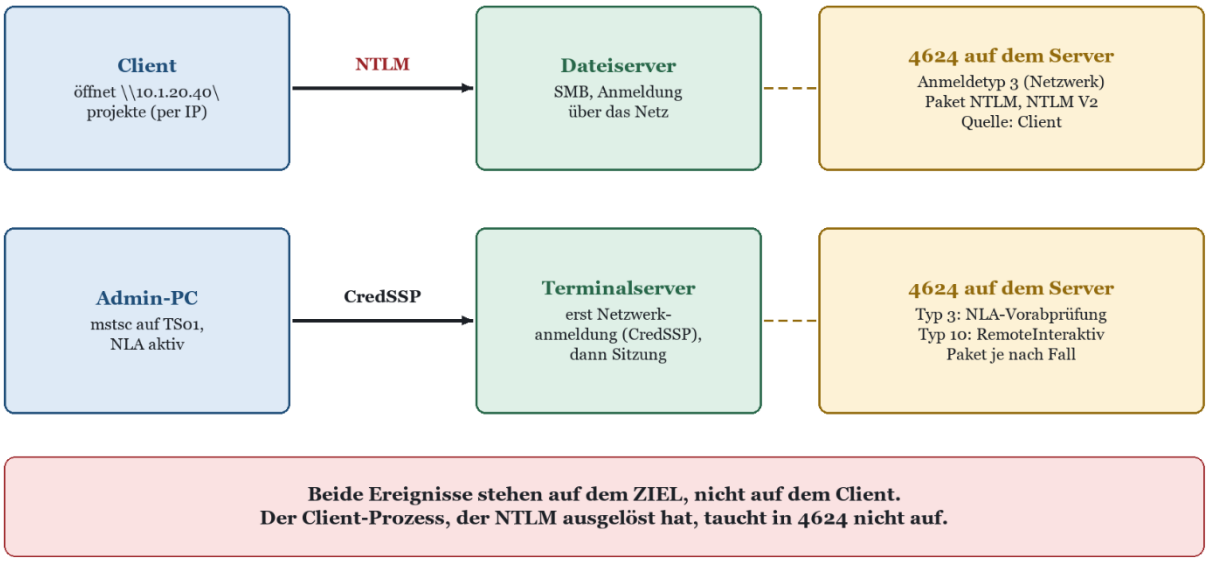
Anmeldetypen 3 und 10: wie NTLM ins Anmeldeprotokoll kommt

Der Anmeldetyp (LogonType) verrät, wie jemand angekommen ist. Für die NTLM-Suche sind zwei Typen die Stammgäste, ein paar weitere tauchen gelegentlich auf.

Anmeldetyp	Bezeichnung	Typischer NTLM-Fall	Bewertung
3	Netzwerk	Zugriff auf Freigaben per IP-Adresse, Drucken, RPC, Dienstkonten von Fachanwendungen, Geräte wie Scanner und NAS	Der Großteil aller NTLM-Treffer
10	RemoteInteraktiv	Remotedesktop-Sitzung; NTLM steckt meist in der vorgelagerten Netzwerkanmeldung über CredSSP	Selten V1, aber wichtig für Admin-Zugänge
8	NetworkCleartext	Anmeldung mit Klartextkennwort, etwa Standardauthentifizierung im IIS	Kein NTLM, aber eigener Prüfpunkt
2 / 11	Interaktiv / zwischengespeichert interaktiv	Lokale Anmeldung am Rechner selbst	Für die V1-Suche kaum relevant
9	NewCredentials	runas /netonly, Zugangsdaten für ausgehende Verbindungen	Bezieht sich auf die lokale Sitzung

Anmeldetyp 3 und 10: wo NTLM auftaucht

Trendforge Digital GmbH, trendforge.local: zwei typische Wege zum Server



Skizze: Namen und Adressen fiktiv

Anmeldetyp 3: der Normalfall für NTLM V1

Fast jeder NTLMv1-Treffer, den du findest, ist Anmeldetyp 3. Ein Client verbindet sich übers Netz, der Server prüft die Antwort und meldet den Erfolg in 4624. Typische Kandidaten bei der Musterwerk GmbH: ein Multifunktionsgerät, das per Scan-to-Folder auf \\fs03\scans schreibt, ein Laborgerät mit eingebautem Windows Embedded, ein Dienstkonto einer Fachanwendung oder ein Client, bei dem jemand vor Jahren LmCompatibilityLevel heruntergesetzt hat. Wenn dein Fund ein Gerät ohne Windows ist, hilft Scan-to-Folder ohne NTLM: Multifunktionsgeräte richtig anbinden; wenn es eine Richtlinie ist, LmCompatibilityLevel richtig setzen: NTLMv2 erzwingen ohne Ausfall.

Anmeldetyp 10: Remotedesktop

Bei Remotedesktop mit Authentifizierung auf Netzwerkebene (NLA) prüft der Server die Anmeldeinformationen schon vor dem Sitzungsaufbau über CredSSP. Dabei entsteht ein 4624 vom Typ 3, danach für die eigentliche Sitzung ein 4624 vom Typ 10. Ob NTLM im Spiel war, siehst du deshalb oft eher an der vorgelagerten Netzwerkanmeldung als am Typ-10-Ereignis selbst. Wer per IP-Adresse auf den Terminalserver zugreift, landet zuverlässig bei NTLM. Die Einzelheiten stehen in RDP, NLA und CredSSP: wann Remotedesktop auf NTLM zurückfällt.

TIPP · Typ 3 plus NTLM V1 plus Computerkonto

Endet das angemeldete Konto auf $, meldet sich ein Computer an, nicht ein Mensch. Das deutet auf Dienste hin, die im Kontext von SYSTEM oder Netzwerkdienst laufen. Den Rechnernamen hast du dann gratis, den Prozess leider nicht.

NTLM V1 filtern: XPath für die Ereignisanzeige und Get-WinEvent

Klickst du in der Ereignisanzeige auf „Aktuelles Protokoll filtern“ und trägst 4624 ein, bekommst du alle Anmeldungen, nicht nur NTLM. Der Reiter „XML“ erlaubt aber eigene Abfragen. Haken bei „Abfrage manuell bearbeiten“ setzen, dann diesen Filter einfügen:

XPath-Filter für die Ereignisanzeige

```
<QueryList>
  <Query Id="0" Path="Security">
```

```
    <Select Path="Security">
      *[System[(EventID=4624)]]
      and *[EventData[Data[@Name='AuthenticationPackageName']='NTLM']]
      and *[EventData[Data[@Name='LmPackageName']='NTLM V1']]
    </Select>
    <Suppress Path="Security">
      *[EventData[Data[@Name='TargetUserSid']='S-1-5-7']]
    </Suppress>
  </Query>
</QueryList>
```

Der Select-Teil holt alle erfolgreichen NTLM-Anmeldungen mit V1, der Suppress-Teil blendet ANONYMOUS LOGON aus. Für den Gegencheck tauschst du „NTLM V1“ gegen „NTLM V2“ oder „LM“, oder du entfernst den Suppress-Block, um die Null Sessions gesondert zu sehen. Der Filter arbeitet auf den XML-Feldern, also unabhängig von der Sprache des Systems: „NTLM V1“ steht im XML immer so, egal ob die Anzeige deutsch oder englisch ist.

WICHTIG · Felder statt Meldungstext

Werte nie den angezeigten Meldungstext aus, sondern die EventData-Felder. Über Windows Event Forwarding weitergeleitete Ereignisse können einen leeren Meldungstext haben, und lokalisierte Texte ändern sich zwischen Sprachen und Versionen. Die XML-Felder bleiben stabil.

Get-WinEvent: eine Hitliste in zehn Zeilen

Mit derselben XPath-Abfrage baust du in PowerShell eine erste Hitliste: wer, von wo, mit welchem Konto, wie oft. Das Beispiel läuft lokal auf einem Server; für Remote-Rechner ergänzt du -ComputerName, sofern die Firewall und deine Rechte das zulassen.

```
$xp = "*[System[(EventID=4624)]] and " +
      "*[EventData[Data[@Name='LmPackageName']='NTLM V1']]"
$ev = Get-WinEvent -LogName Security -FilterXPath $xp -MaxEvents 50000 -ErrorAction
SilentlyContinue

$ev | ForEach-Object {
    $d = @{}
    ([xml]$_.ToXml()).Event.EventData.Data | ForEach-Object { $d[$_.Name] = $_.'#text' }
    [pscustomobject]@{
        Konto     = "$($d.TargetDomainName)\$($d.TargetUserName)"
        Quelle    = $d.WorkstationName
        IP        = $d.IpAddress
        Typ       = $d.LogonType
        Schlüssel = $d.KeyLength
        Anonym    = ($d.TargetUserSid -eq 'S-1-5-7')
    }
} | Group-Object Konto, Quelle, IP, Typ, Anonym |
    Sort-Object Count -Descending |
    Select-Object Count, Name -First 25
```

Das Ergebnis ist eine nach Häufigkeit sortierte Liste von Kombinationen aus Konto, Quelle, Adresse, Anmeldetyp und dem Merker für anonyme Anmeldungen. Die ersten fünf Zeilen erklären meist neunzig Prozent des Volumens. Weitere Rezepte, etwa für mehrere Server parallel oder den Export nach CSV, sammelt NTLM-Ereignisse mit PowerShell auswerten: Get-WinEvent-Rezepte. Fehlgeschlagene Versuche mit denselben Feldern findest du in 4625; wie du deren Statuscodes deutest, beschreibt Fehlercodes 0xC000006D und Co.: fehlgeschlagene NTLM-Anmeldungen deuten.

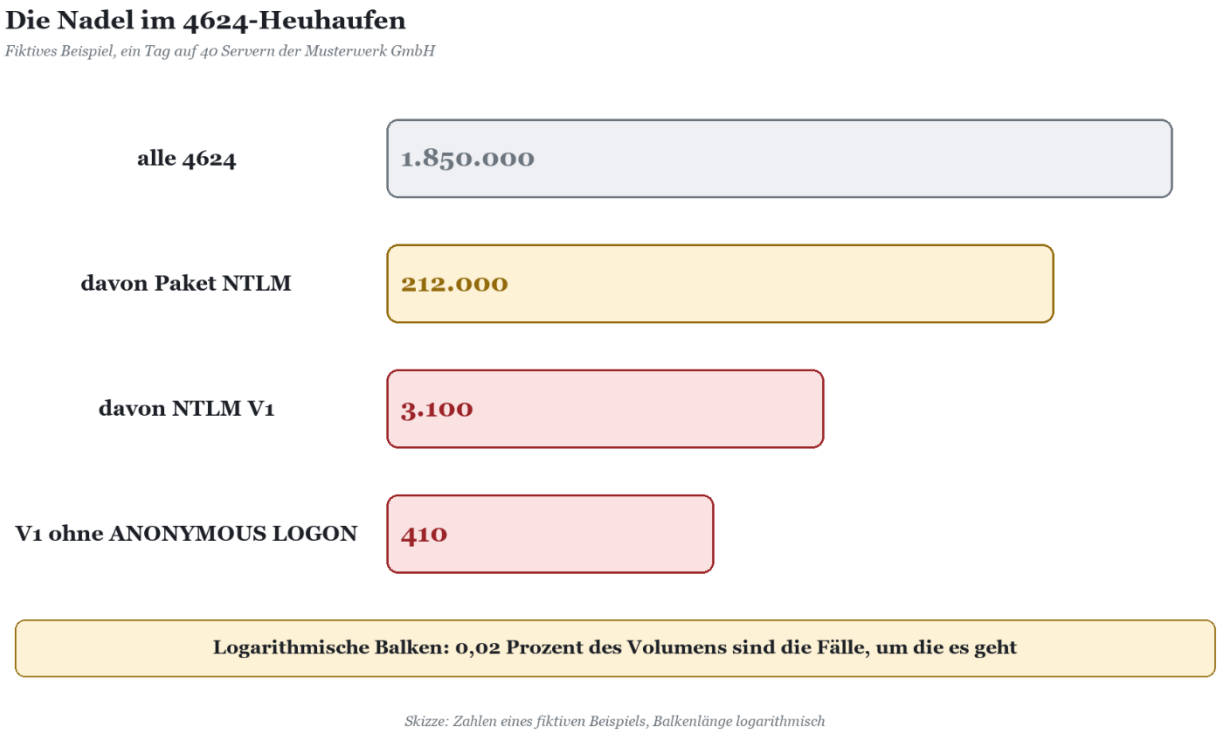
AUS DER PRAXIS · Die Steuerkanzlei und der Scanner aus dem Keller

Bei der Sparfuchs & Partner Steuerberatungs GmbH (sparfuchs.local) zeigt der XPath-Filter auf dem Dateiserver jeden Werktag rund 180 Anmeldungen mit „NTLM V1“, Anmeldetyp 3, Konto svc-scan, Quelladresse 10.10.5.21, Arbeitsstationsname leer. Die Rückwärtsauflösung liefert nichts, das Inventar auch nicht.

Am Ende führt ein Blick in die DHCP-Reservierungen zu einem Multifunktionsgerät im Archivraum, Firmware von 2016. Das Gerät kann laut Hersteller NTLMv2, war aber nie umgestellt. Zehn Minuten im Webinterface, und die Zeile verschwindet aus der Hitliste. Gesucht hat man vorher zwei Tage.

Warum das Sicherheitsprotokoll für die ganze Domäne zu laut ist

Auf einem einzelnen Server funktioniert das alles erstaunlich gut. Domänenweit wird es unangenehm, und zwar aus Gründen, die nichts mit deinem PowerShell-Können zu tun haben.



Skizze: Zahlen eines fiktiven Beispiels, Balkenlänge logarithmisch

Hürde	Was passiert	Folge für die V1-Suche
Volumen	4624 entsteht bei jeder Anmeldung, auch bei Kerberos, Computerkonten, Diensten und geplanten Aufgaben	Die NTLMv1-Treffer sind ein winziger Bruchteil; Transport und Speicher kosten trotzdem für alles
Überschreiben	Das Sicherheitsprotokoll ist begrenzt und rotiert auf viel genutzten Servern schnell	Seltene Quellen, etwa ein Monatsabschluss-Job, sind weg, bevor du sie suchst
Verteilung	4624 steht auf dem Ziel, also auf jedem Server und jedem DC einzeln	Ohne zentrale Sammlung fragst du Hunderte Protokolle ab
Blinder Fleck Client	4624 kennt den Zielrechner und die Quelle, aber nicht den Prozess auf dem Client	Du weißt, dass CL-EK-0412 V1 schickt, aber nicht, welches Programm
Kein Warum	4624 enthält keine Begründung, warum NTLM statt Kerberos gewählt wurde	Fehlender SPN, IP-Zugriff oder Altgerät musst du selbst erraten
Rauschen	Anonyme Anmeldungen, Computerkonten und Dienste mischen sich in dieselben Treffer	Ohne sauberes Gruppieren wirkt die Lage schlimmer oder harmloser, als sie ist

Dazu kommt ein organisatorisches Problem: Wer 4624 von allen Servern per Windows Event Forwarding einsammelt, flutet den Collector mit Millionen Ereignissen, von denen er 99,9 Prozent nie anschaut. Sinnvoller ist es, gezielt die NTLM-Ereignisse zu sammeln, die genau für diesen Zweck gebaut wurden: 8001 bis 8004 aus dem klassischen NTLM-Auditing und seit den Updates ab 13.10.2026 die erweiterten Ereignisse 4020 bis 4025 und 4030 bis 4033. Die liefern das Feld NtlmVersion gleich mit, dazu Prozess, Ziel und Begründung. Wie du sie einschaltest, steht in Erweitertes NTLM-Auditing einschalten, eine fertige Gruppenrichtlinie liefert das NTLM-Audit-GPO-Skript, und das Einsammeln beschreibt NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding.

Merkmal	4624 (Sicherheit)	4776 (DC)	4020 bis 4023 (NTLM, erweitert)
NTLM-Version	ja, LmPackageName	nein	ja, NtlmVersion
Quelle	Arbeitsstation und IP	Arbeitsstation	ja, inkl. Client-IP auf Serverseite
Zielrechner	ja, der protokollierende Rechner	nein	ja, TargetMachine
Prozess auf dem Client	nein	nein	ja, ProcessName (4020/4021)
Begründung	nein	nein	ja, NtlmUsageReason
Rauschen	sehr hoch	hoch	gering, nur NTLM

4624 bleibt trotzdem nützlich: als schnelle Stichprobe auf einem verdächtigen Server, für Rechner, auf denen das erweiterte Auditing noch nicht läuft, und als Gegenprobe nach einer Umstellung. Für die Prüfung am Domain Controller selbst gibt es mit Ereignis 4776 auf dem Domain Controller: NTLM-Anmeldungen im Sicherheitsprotokoll ein Schwester-Ereignis, das noch weniger verrät, dafür aber zentral anfällt. Und bei den Begründungstexten gilt, was in NTLM-Reason-IDs erklärt steht: Maßgeblich ist der Text in NtlmUsageReason, die Nummer ist nur ein Hinweis.

WICHTIG · Geräte ohne Ereignisprotokoll

Der Scanner, das NAS, die Laborsteuerung: Sie schreiben kein 4020. Du siehst sie nur auf der Gegenseite, also im 4624 oder 4022 des Servers, auf den sie zugreifen. Für Geräte, die gar nicht mit einem Windows-Server reden, hilft nur ein Netzwerkmitschnitt. Mehr dazu:

› NAS, Drucker und Scanner: NTLM bei Geräten ohne Ereignisprotokoll

Die NTLMv1-Hitliste mit dem NTLM Diagnostiker

Die Schritte bis hierher kosten pro Server ein paar Minuten. Bei fünf Servern ist das ein Vormittag, bei zweihundert Servern und drei Domain Controllern eine Woche, und am Ende hast du immer noch keine Prozesse und keine Begründungen. Genau diese Lücke schließt der NTLM Diagnostiker: Er sammelt die NTLM-Ereignisse direkt vom Domain Controller, über einen vorhandenen Windows Event Collector, per Direktabfrage oder per Datei-Import, wertet die Felder aus und fasst gleichartige Verbindungen nach Ursache, Prozess und Ziel zusammen. Er arbeitet ausschließlich lesend; an deiner Umgebung ändert er nichts.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Von „27 Verbindungen mit NTLMv1“ zur Liste der Schuldigen

Übersicht öffnen: Die Kennzahlen zeigen sofort, wie viele Verbindungen NTLMv1 benutzen, daneben die Top-10-Verursacher mit Prozess, Ursache, Kategorie, Quellen und Anmeldungen und unten die

Readiness-Ampel. Gleichartige Verbindungen sind bereits zusammengefasst, ANONYMOUS LOGON und echte Kennwortanmeldungen laufen nicht durcheinander.

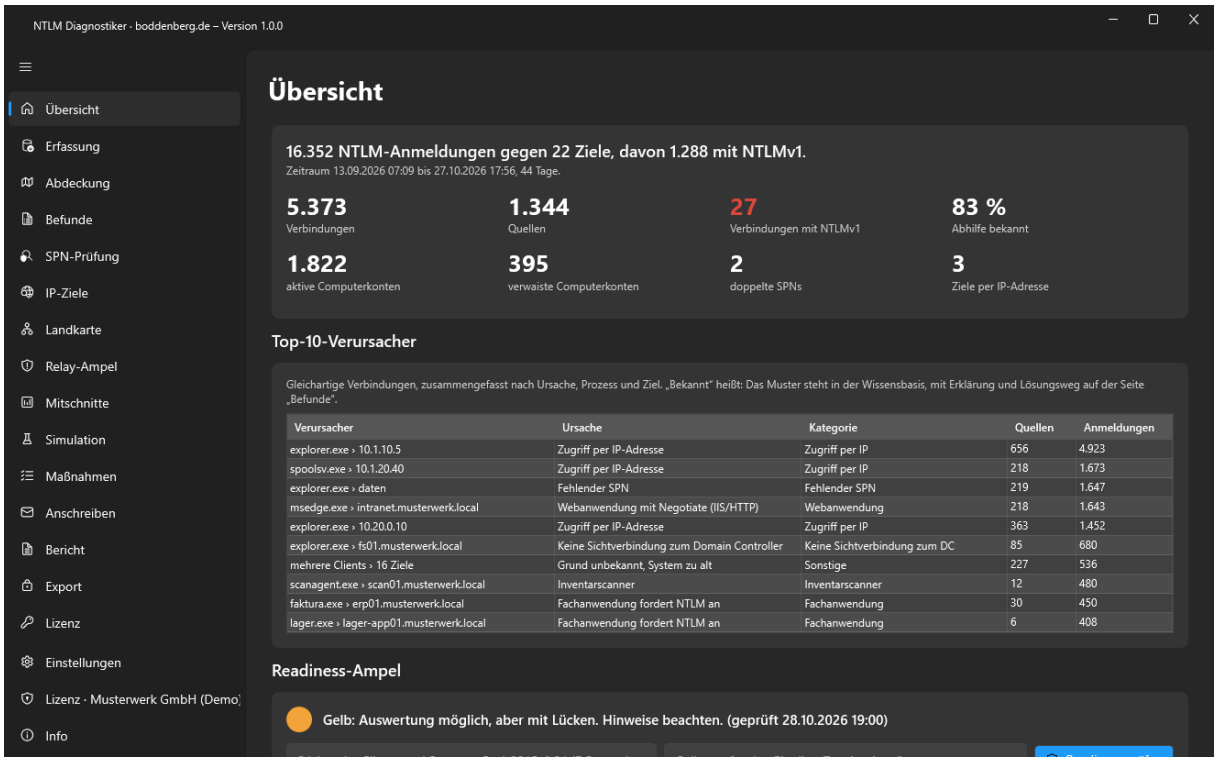
NTLMv1-Hitliste aufrufen: Sie listet jede Quelle, die noch V1 schickt, mit Ziel, Konto und Häufigkeit. Weil die Auswertung auch die Client-Ereignisse kennt, steht dort, wo verfügbar, der auslösende Prozess. Genau die Spalte, die dir 4624 schuldig bleibt.

Ursache lesen: Die Ursachen-Engine wertet den Begründungstext aus NtlmUsageReason aus und verknüpft ihn mit der Wissensbasis bekannter Verursacher, samt Erklärung und Lösungsweg.

Lücken prüfen: Die Abdeckungskarte zeigt je OU und Betriebssystem, welche Rechner Ereignisse liefern und welche schweigen. Für Geräte ohne Ereignisprotokoll gibt es den Mitschnitt-Import (pcap/pcapng).

Nachweisen: Mit dem Hersteller-Anschreiben gehen Prozess, Ziel und Häufigkeit als Beleg an den Anbieter, und das Maßnahmen-Board zeigt mit der Verlaufskurve, ob die V1-Zahl wirklich sinkt.

› NTLM Diagnostiker



Hier siehst du in der Übersicht, wie viele Verbindungen noch NTLMv1 benutzen, und welche Verursacher am häufigsten auftreten (Demodaten).

Zum Ausprobieren reicht die kostenlose Edition Express: Sie liefert unbegrenzt einen Fünf-Minuten-Befund direkt vom DC mit Readiness-Ampel, Abdeckungskarte, Top-10-Verursachern, Hinweisen aus der Wissensbasis und einem NTLMv1-Alarm mit Anzahl und Top 5, dazu einen Kurzbefund als PDF. Einmal pro Domäne kannst du sieben Tage lang fast den ganzen Funktionsumfang testen; lizenziert wird pro aktivem Computerkonto für 18 Monate, für beliebig viele Domänen. Eine Phase-3-Bereitschaftsprüfung und ein Kerberos-Gegencheck sind geplant.

Wenn du die V1-Quellen lieber gemeinsam mit jemandem jagst, der die üblichen Verdächtigen kennt, hilft dir die Beratung zur NTLM-Ablösung. Soll dein Team Anmeldeprotokoll und NTLM-Ereignisse künftig selbst lesen, ist die Schulung zum NTLM Diagnostiker der kürzere Weg. Wie die Kerberos-Seite funktioniert, auf die du am Ende umstellst, erklärt Microsoft Kerberos.

FAQ zu 4624 und NTLM V1

Wo genau steht in 4624, ob NTLM V1 oder V2 benutzt wurde?

Im Abschnitt „Detaillierte Authentifizierungsinformationen“ im Feld „Paketname (nur NTLM)“, im XML LmPackageName. Mögliche Werte sind „NTLM V1“, „NTLM V2“ und „LM“.

Warum steht bei manchen Anmeldungen nur ein Bindestrich?

Weil das Feld nur befüllt wird, wenn das Authentifizierungspaket NTLM ist. Bei Kerberos und bei Negotiate, das sich für Kerberos entschieden hat, bleibt es leer.

Ist jedes 4624 mit NTLM V1 ein Sicherheitsproblem?

Jedes ist eine Altlast, aber nicht jedes gleich gefährlich. Anmeldungen von ANONYMOUS LOGON sind Null Sessions ohne Kennwort und gehören in eine eigene Liste. Kritisch sind V1-Anmeldungen echter Benutzer-, Dienst- und Computerkonten.

Auf welchem Rechner muss ich suchen?

Auf dem Ziel, also dem Rechner, an dem die Anmeldung stattfindet. Ein Client, der V1 schickt, hinterlässt das 4624 auf dem Dateiserver, nicht bei sich selbst.

Welche Überwachungsrichtlinie brauche ich?

Die erweiterte Unterkategorie „Anmelden überwachen“ in der Kategorie „Anmelden/Abmelden“, mindestens für Erfolg. Sie ist auf Windows-Servern üblicherweise bereits aktiv; prüfen kannst du das mit auditpol /get /category:* und einem Blick auf die Zeile „Anmelden“.

Warum sehe ich NTLM V1, obwohl LmCompatibilityLevel auf 5 steht?

Der Wert auf dem Server bestimmt, was der Server selbst sendet und annimmt. Die Version im 4624 kommt vom Client. Steht der Wert auf dem Domain Controller und den Servern korrekt, werden V1-Antworten abgelehnt; tauchen sie trotzdem erfolgreich auf, prüf die Einstellung dort, wo die Anmeldung tatsächlich geprüft wird. Einzelheiten in LmCompatibilityLevel richtig setzen: NTLMv2 erzwingen ohne Ausfall.

Taucht NTLM auch bei WLAN-Anmeldungen in 4624 auf?

Nicht als Anmeldung am Dateiserver, aber MSCHAPv2 über NPS basiert auf NTLM-Mechanismen und wird deshalb gern übersehen. Die Zusammenhänge beschreibt MSCHAPv2, NPS und WLAN: die versteckte NTLM-Abhängigkeit.

Kann ich 4624 domänenweit per Event Forwarding sammeln?

Technisch ja, sinnvoll selten. Das Volumen ist enorm, und der Informationsgewinn für die NTLM-Ablösung ist kleiner als bei den eigens dafür gebauten NTLM-Ereignissen. Sammle besser diese und nimm 4624 für Stichproben.

Wo steht das bei Microsoft?

In der Ereignisreferenz 4624(S): An account was successfully logged on. Dort findest du Event-XML, Anmeldetypen und die Beschreibung von Paketname und Schlüssellänge.

Fazit: Das Gästebuch kennt die Version, nicht den Täter

Ereignis 4624 beantwortet die Frage nach NTLM V1 oder V2 zuverlässig: Authentifizierungspaket NTLM, Paketname „NTLM V1“, fertig. Mit einem XPath-Filter und zehn Zeilen PowerShell hast du auf einem Server in Minuten eine Hitliste aus Konto, Quelle und Anmeldetyp. Trenn die anonymen Anmeldungen ab, achte auf die Schlüssellänge, und du weißt, wie ernst die Lage auf diesem Rechner ist.

Für die ganze Domäne taugt das Sicherheitsprotokoll aber nur als Stichprobe. Es ist zu laut, zu verteilt, zu schnell überschrieben, und es verschweigt Prozess und Begründung. Die belastbare Antwort kommt aus den NTLM-Ereignissen, zentral gesammelt und nach Ursache gruppiert, ob mit eigenen Skripten oder mit dem Diagnostiker. Der Pförtner schreibt brav alles auf. Die Ermittlung musst du trotzdem selbst führen, und zwar bevor der Stichtag die Tür für alle zumacht. Eine Übersicht der Prüfpunkte bis dahin liefert Checkliste vor dem NTLM-Stichtag: 25 Prüfpunkte.

WEITERLESEN · Weiter in dieser Serie

› Ereignis 4776 auf dem Domain Controller: NTLM-Anmeldungen im Sicherheitsprotokoll
› LmCompatibilityLevel richtig setzen: NTLMv2 erzwingen ohne Ausfall
› NTLM-Ereignisse mit PowerShell auswerten: Get-WinEvent-Rezepte
› Fehlercodes 0xC000006D und Co.: fehlgeschlagene NTLM-Anmeldungen deuten
› Anonyme Anmeldungen und Null Sessions: NTLM-Altlasten aufräumen
› RDP, NLA und CredSSP: wann Remotedesktop auf NTLM zurückfällt
› Erweitertes NTLM-Auditing einschalten
› NTLM-Reason-IDs erklärt