NAS, Drucker und Scanner: NTLM bei Geräten ohne Ereignisprotokoll



WISSEN
Wie der NTLM Diagnostiker Ereignisse und Mitschnitte zusammenführt und stille Geräte sichtbar macht.
› NTLM Diagnostiker

BERATUNG
NAS, Multifunktionsgeräte und Medizintechnik bewerten, Kerberos einrichten, Ausnahmen sauber begründen.
› Beratung zur NTLM-Ablösung

SCHULUNG
Serversicht, DC-Sicht und Mitschnitt lesen lernen, damit dein Team die stummen Zeugen selbst befragt.
› Schulung zum NTLM Diagnostiker

Es gibt in jedem Netz eine Gruppe von Geräten, die sich bei der NTLM-Ablösung verhält wie der Onkel auf der Familienfeier, der nie etwas sagt, aber am Ende das Buffet leer gegessen hat. Das NAS im Keller, das seit 2017 die Sicherungen schluckt. Das Multifunktionsgerät im zweiten Stock, das Lieferscheine auf eine Freigabe scannt. Das Ultraschallgerät, dessen Betriebssystem älter ist als die jüngste Assistenzärztin. Und der Linux-Server, den ein Kollege eingerichtet hat, der inzwischen in Portugal Surfkurse gibt. Alle diese Geräte sprechen NTLM. Keines davon schreibt ein einziges Ereignis in ein Windows-Protokoll.

Wer nach nas ntlm kerberos sucht, hat das Problem meist schon gespürt: Die Auswertung der Ereignisse sieht ordentlich aus, die Kurve fällt, und trotzdem weiß niemand, was am Stichtag tatsächlich ausfällt. Denn Windows protokolliert nur, was ein Windows-System selbst erlebt. Ein Gerät ohne Ereignisprotokoll fällt bei einer Auswertung, die nur Ereignisse kennt, durch alle Raster. Es fällt erst wieder auf, wenn es nicht mehr funktioniert.

Der Zeitdruck ist bekannt: Seit dem Windows-Update vom 13.10.2026 blockieren Windows 11 ab 24H2 und Windows Server 2025 Single Sign-on mit NTLMv1 standardmäßig, gesteuert über den Registrierungswert BlockNtlmv1SSO und sichtbar in den Ereignissen 4024 und 4025. Phase 2 bringt IAKerb und ein lokales KDC, und mit der nächsten Windows-Server-Version ist NTLM standardmäßig abgeschaltet. Was das für die Windows-Seite heißt, steht in NTLMv1 blockiert: was seit Oktober 2026 nicht mehr geht. Dieser Beitrag kümmert sich um die andere Seite: um die Geräte, die nichts protokollieren, und darum, wie du sie trotzdem findest.

Du erfährst, warum NAS, Drucker, Scanner, Medizintechnik und Linux-Systeme im Windows-Audit unsichtbar oder nur halb sichtbar sind, welche drei Fundorte dir trotzdem bleiben, wie du die Lücke mit einem Mitschnitt schließt und welche Lösungen in der Praxis tragen: Firmware, Kerberos-Konfiguration, SMB-Einstellungen und, wenn alles andere scheitert, der Austausch.

FAKTEN · Stille Geräte und NTLM auf einen Blick

Erweitertes NTLM-Auditing gibt es laut Microsoft KB5064479 nur auf Windows 11 ab 24H2, Windows Server 2025 sowie Windows Server 2022 und 2019 mit Updates ab dem 13.10.2026. NAS, Multifunktionsgeräte, Linux und eingebettete Systeme schreiben diese Ereignisse grundsätzlich nicht.

Clientsicht 4020/4021, Serversicht 4022/4023, Domain Controller 4030 bis 4033, jeweils im Protokoll Microsoft-Windows-NTLM/Operational. Die Reason ID (0 bis 11) steht nur in der Clientsicht, also nur dann, wenn ein Windows-System der Anrufer ist.

Klassische Restrict-NTLM-Überwachung 8001 bis 8004 funktioniert auch auf älteren Windows-Versionen, liefert aber keine Reason ID.

Ist das Gerät der Anrufer, siehst du es auf dem Windows-Server (4022/4023, 8002, 4624) und bei Domänenkonten zusätzlich auf dem Domain Controller (8004, 4030 bis 4033, 4776).

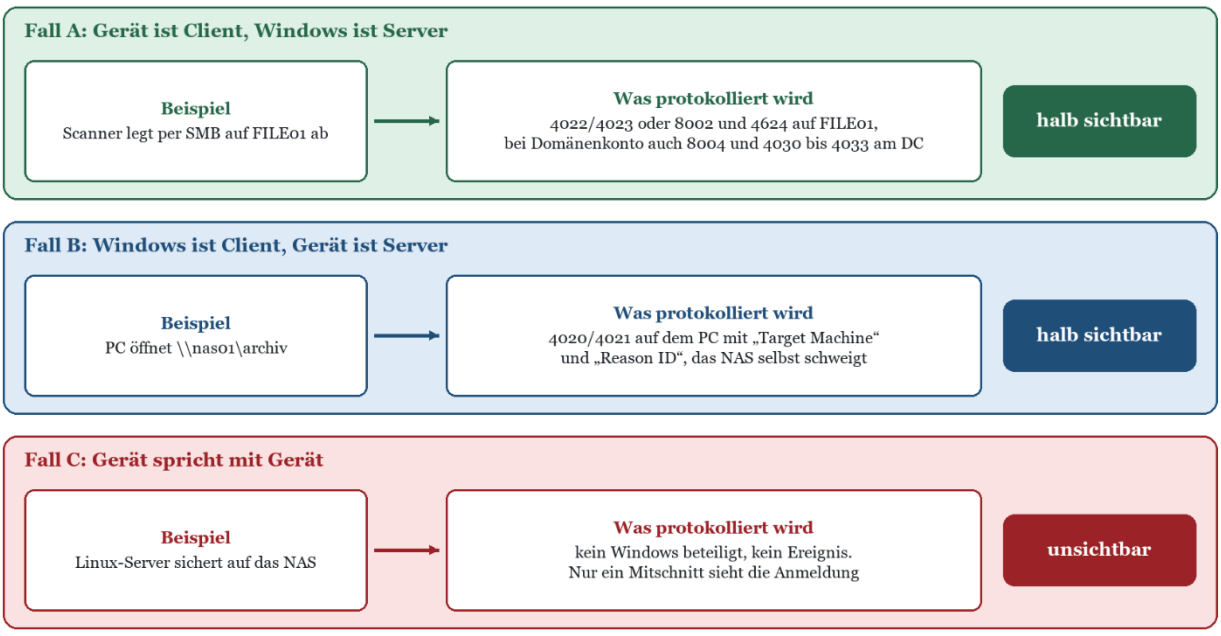
Sprechen zwei Nicht-Windows-Geräte miteinander, gibt es kein einziges Windows-Ereignis. Dann hilft nur ein Netzwerkmitschnitt.

Warum stille Geräte im Windows-Audit fehlen

Das Missverständnis beginnt mit einem harmlos klingenden Satz: „Wir haben das NTLM-Auditing aktiviert.“ Aktiviert hast du es auf Windows-Systemen, per Gruppenrichtlinie, und genau dort wirkt es. Ein NAS liest keine Gruppenrichtlinien. Ein Multifunktionsgerät hat kein Protokoll Microsoft-Windows-NTLM/Operational. Ein Linux-Server protokolliert, wenn überhaupt, in sein eigenes Journal, und niemand hat ihn je gebeten, das an den Collector zu schicken. Das Auditing ist also nicht kaputt. Es ist nur höflich und spricht ausschließlich mit Systemen, die es kennt.

Halb sichtbar, ganz unsichtbar: wer protokolliert was?

Entscheidend ist, auf welcher Seite der Verbindung ein Windows-System sitzt.



Skizze: vereinfacht. Erweiterte Ereignisse nur auf Systemen laut KB5064479

Die Skizze zeigt die drei Fälle, auf die es ankommt. Ist das Gerät der Anrufer und Windows der Angerufene, siehst du die Anmeldung auf dem Windows-Server. Ist es umgekehrt, siehst du sie auf dem Windows-Client, der das Gerät anspricht. Und wenn kein Windows beteiligt ist, siehst du gar nichts. „Halb sichtbar“ heißt dabei: Du siehst eine Seite der Verbindung, aber nie die Ursache auf der Geräteseite. Warum das NAS keine Kerberos-Tickets annimmt, steht in keinem Windows-Ereignis.

NAS-Systeme: Samba, lokale Konten und die IP-Adresse

Die meisten NAS-Systeme im Mittelstand basieren auf Samba. Samba kann Kerberos, und zwar seit vielen Jahren ordentlich, sofern das NAS als Mitglied der Domäne beigetreten ist, ein Computerkonto mit passenden SPNs besitzt und unter seinem DNS-Namen angesprochen wird. In der Praxis scheitert es fast immer an einem dieser drei Punkte. Das NAS wurde nie in die Domäne aufgenommen, weil es „nur für die Sicherung“ gedacht war, und arbeitet mit lokalen Konten. Oder es ist Mitglied, wird aber überall als \\10.20.1.50\backup angesprochen. Oder es wurde umbenannt, und der alte Name lebt als DNS-Alias ohne SPN weiter.

Die Folgen siehst du auf der Windows-Seite: Clients, die auf das NAS zugreifen, melden 4020 mit Reason ID 7 bei IP-Adressen, Reason ID 6 bei Namen ohne SPN und Reason ID 2, wenn sie sich mit einem lokalen Konto des NAS anmelden. Das ist die halbe Sichtbarkeit aus Fall B. Wo das NAS selbst der Anrufer ist, etwa bei einer Replikation auf einen Windows-Dateiserver, bist du in Fall A. Und wenn das NAS auf ein zweites NAS repliziert, in Fall C. Wie du IP-Zugriffe umstellst, beschreibt NTLM wegen IP-Adresse: Laufwerke und Skripte auf DNS-Namen umstellen; fehlende SPNs behandelt Reason-ID 6: wenn der Zielname nicht auflösbar ist.

Multifunktionsgeräte und Scanner: Scan to Folder

Das Multifunktionsgerät ist der Klassiker unter den stillen Zeugen. Die Funktion „Scan to Folder“ legt Dokumente per SMB auf einer Windows-Freigabe ab. Dazu meldet sich das Gerät mit einem Konto an, das jemand vor Jahren in das Webinterface getippt hat, häufig mit einer IP-Adresse als Ziel. Viele Geräte können dabei Kerberos, wenn man es ihnen erklärt: Realm, KDC und eine halbwegs korrekte Uhrzeit. Ohne diese Angaben nehmen sie NTLM, ältere Firmware gern auch NTLMv1 und SMB1. Dazu kommen Adressbuchabfragen per LDAP, die sich mit einem einfachen Bind oder mit NTLM gegen den Domain Controller anmelden.

Gedruckt wird dagegen meist unproblematisch: Windows-Clients drucken über den Druckserver, und der spricht mit dem Gerät in der Regel über Druckprotokolle ohne Windows-Anmeldung. Ärger machen eher Druckserver, die selbst per IP-Adresse auf Freigaben zugreifen, und Verwaltungsprogramme der Hersteller, die Geräte per SMB oder HTTP mit NTLM abfragen.

Medizintechnik: validiert, eingefroren, unantastbar

In Kliniken kommt eine besondere Spezies hinzu: Geräte mit eingebettetem Windows oder Linux, deren Software als Medizinprodukt zugelassen ist. Ein Update ist dort keine Frage der Lust, sondern der Zulassung, und die Konfiguration darf oft nur der Hersteller ändern. Läuft ein solches Gerät auf einer alten Windows-Version, schreibt es zwar Ereignisse, aber keine erweiterten NTLM-Ereignisse. Steht es in einem eigenen Netzsegment ohne Domänenbeitritt, meldet es sich mit lokalen Konten an Archivsystemen an. Die Geräte sind im Audit also nicht ganz stumm, sie reden nur in einer Sprache, die das erweiterte Auditing nicht versteht. Den Klinikalltag mit Labor, Bildgebung und Fachanwendungen behandelt NTLM in der Klinik: Medizintechnik, Labor und Fachanwendungen.

Linux-Systeme: cifs-Mounts und Skripte

Linux-Server greifen über cifs-utils oder smbclient auf Windows-Freigaben zu. Ein Eintrag in /etc/fstab mit Benutzername und Kennwortdatei ergibt eine NTLM-Anmeldung, eine Einbindung

mit der Option sec=krb5 und einem gültigen Ticket dagegen Kerberos. Welche Variante auf deinen Servern läuft, verrät kein Windows-Ereignis direkt, nur die Serversicht der Gegenseite. Dasselbe gilt für Skripte, Monitoring-Agenten und Backup-Werkzeuge, die mit Benutzername und Kennwort hantieren. Sind Linux-Systeme per realm oder sssd in die Domäne aufgenommen, ist Kerberos grundsätzlich vorhanden; es muss nur jemand die Einbindungen darauf umstellen.

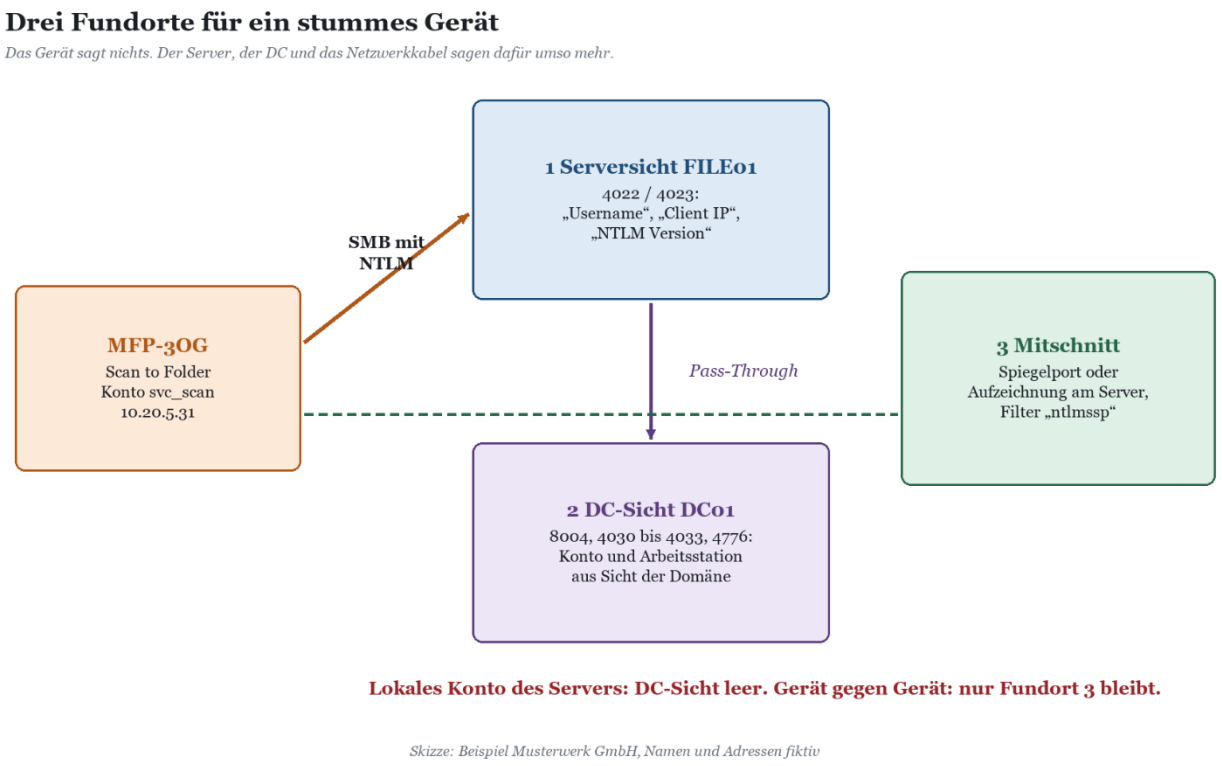
Geräteklasse	Typische NTLM-Ursache	Sichtbar wo?	Erste Maßnahme
NAS (Samba-basiert)	kein Domänenbeitritt, lokale Konten, Zugriff per IP	4020 auf Windows-Clients, Mitschnitt	Domänenbeitritt, DNS-Namen, SPN prüfen
Multifunktionsgerät	Scan to Folder mit IP und Konto, Kerberos nicht konfiguriert	4022/4023, 8002, 4624 auf dem Ziel, 8004 am DC	Kerberos im Webinterface, Firmware
Dokumentenscanner	Hersteller-Software mit NTLM, alte Treiber	Serversicht, Mitschnitt	Software aktualisieren, Hersteller fragen
Medizintechnik	eingefrorene Firmware, lokale Konten, alte Windows-Version	Serversicht, 8001 bis 8004 auf Altsystemen, Mitschnitt	Hersteller, Netztrennung, Ausnahme
Linux-Server	cifs-Mount mit Kennwortdatei, Skripte	Serversicht, DC-Sicht	sec=krb5, Domänenbeitritt per realm oder sssd
Gerät gegen Gerät	beliebig	nur im Mitschnitt	Mitschnitt, dann Geräteanalyse

WARNUNG · Ein stilles Gerät ist kein sauberes Gerät

Die gefährlichste Zeile in jeder NTLM-Auswertung ist die, die fehlt. Ein Gerät ohne Ereignisse sieht in der Statistik exakt so aus wie ein Gerät ohne NTLM. Wenn du am Stichtag die Restrict-NTLM-Richtlinie auf Verweigern stellst, fragt niemand mehr nach Protokollen. Dann fragt nur noch die Buchhaltung, warum seit acht Uhr keine Rechnungen mehr eingescannt werden.

Stille Geräte trotzdem finden: Server, DC und Mitschnitt

Ein Gerät, das selbst nichts sagt, lässt sich über seine Gesprächspartner überführen. Dafür hast du drei Fundorte. Die ersten beiden nutzen das, was Windows ohnehin protokolliert, der dritte schaut direkt aufs Kabel.



Fundort 1: die Serversicht mit 4022 und 4023

Meldet sich ein Gerät an einem Windows-Server an, schreibt der Server Ereignis 4022, bei unsicheren Varianten wie NTLMv1 die Warnung 4023. Voraussetzung ist das erweiterte Auditing auf dem Server, eingeschaltet per Gruppenrichtlinie wie in Erweitertes NTLM-Auditing einschalten: Schritt für Schritt beschrieben; die passende Richtlinie samt Überwachung der klassischen Ereignisse legt dir das NTLM-Audit-GPO-Skript an. Im Meldungstext stehen unter „Remote Client Information“ das Konto, der vom Gerät gemeldete Rechnername unter „Client Machine“ und die Herkunft unter „Client IP“. Der Rechnername ist eine Selbstauskunft und bei Geräten oft leer oder ein Werkseinstellungsname. Verlässlich ist die IP-Adresse. Unter „NTLM Version“ siehst du, ob das Gerät noch NTLMv1 spricht. Alle Felder erklärt Ereignis 4022 und 4023: eingehende NTLM-Anmeldungen auf Servern.

Weil die Serversicht keine Reason ID enthält, suchst du nach Mustern: Konten, die nach Gerätefunktion klingen, IP-Adressen aus Druckersegmenten, leere Rechnernamen. Dieser Block zählt eingehende Anmeldungen nach IP-Adresse, Konto und Version und liest dazu den Meldungstext, weil die Feldnamen der EventData nicht dokumentiert sind:

```
$ev = Get-WinEvent -LogName 'Microsoft-Windows-NTLM/Operational' `
  -FilterXPath '*[System[(EventID=4022 or EventID=4023)]]' -MaxEvents 20000
$ev | ForEach-Object {
  $m = $_.Message
  [pscustomobject]@{
    IP      = ([regex]::Match($m, 'Client IP:\s*(\S+)')).Groups[1].Value
    Konto   = ([regex]::Match($m, 'Username:\s*(\S+)')).Groups[1].Value
    Version = ([regex]::Match($m, 'NTLM Version:\s*(\S+)')).Groups[1].Value
  }
} | Group-Object IP, Konto, Version | Sort-Object Count -Descending |
  Select-Object Count, Name -First 30
```

Prüfe die Suchmuster an einem echten Ereignis deines Servers, bevor du dich auf die Zahlen verlässt. Auf Servern ohne erweitertes Auditing bleiben die klassischen Quellen: 8002 aus der Restrict-NTLM-Überwachung für eingehenden Verkehr und Ereignis 4624 im Sicherheitsprotokoll

mit „Authentication Package: NTLM“ und der Zeile „Package Name (NTLM only)“, die NTLM V1 und NTLM V2 unterscheidet. Schnell und ohne PowerShell geht das mit wevtutil:

```
wevtutil qe Security /q:"*[System[(EventID=4624)] and
EventData[Data[@Name='AuthenticationPackageName']='NTLM']]" /c:20 /rd:true /f:text
```

Fundort 2: die DC-Sicht

Meldet sich ein Gerät mit einem Domänenkonto an, muss der Server die Anmeldung beim Domain Controller prüfen lassen. Dort entstehen die Ereignisse 4030 bis 4033 aus dem erweiterten Auditing sowie 8004 aus der klassischen Überwachung, und im Sicherheitsprotokoll 4776 für die Prüfung der Anmeldedaten. Der Vorteil: Du musst nicht jeden Dateiserver abfragen, die Domain Controller sehen alle Domänenanmeldungen zentral. Der Nachteil: Lokale Konten des Zielservers oder des NAS tauchen dort nie auf, und den Grund für NTLM erfährst du auch hier nicht. Welche Felder die DC-Ereignisse enthalten, steht in NTLM auf dem Domain Controller: Ereignisse 4030 bis 4033 und 8004.

Fundort 3: der Mitschnitt

Für Fall C, Gerät gegen Gerät, und für alle Server ohne Auditing bleibt der Blick aufs Kabel. Ein Mitschnitt an einem Spiegelport vor dem NAS oder direkt auf einem Windows-Dateiserver zeigt jede NTLM-Aushandlung im Klartext der Metadaten: Konto, Domäne, Rechnername, Ziel und die verwendete Version. In Wireshark genügt der Anzeigefilter ntlmssp, für die eigentlichen Anmeldungen der Filter auf den Nachrichtentyp 3. Auf Windows-Servern ohne Wireshark-Installation zeichnet das Bordmittel pktmon auf und wandelt die Aufzeichnung anschließend in das pcapng-Format um:

```
pktmon filter add SMB -p 445
pktmon start --capture --pkt-size 0 --file-name C:\Temp\smb.etl
# ... einen Arbeitstag laufen lassen, dann:
pktmon stop
pktmon etl2pcap C:\Temp\smb.etl --out C:\Temp\smb.pcapng

# Wireshark-Anzeigefilter:
ntlmssp.messagetype == 0x00000003                       # alle NTLM-Anmeldungen
ntlmssp.messagetype == 0x00000003 && !ntlmssp.ntlmv2_response   # Kandidaten für NTLMv1
```

Zwei Grenzen solltest du kennen. Verschlüsselte Verbindungen wie HTTPS, LDAPS oder RDP mit TLS sieht kein Mitschnitt von innen. Und ein Mitschnitt enthält personenbezogene Daten, also Konten, Rechnernamen und unter Umständen Inhalte; kläre vorher, wer aufzeichnen darf und wie lange die Datei liegen bleibt, siehe NTLM-Audit, Datenschutz und Betriebsrat: was du beachten musst. Wie du Aufzeichnungspunkt, Filter und Dauer sinnvoll wählst, erklärt ausführlich NTLM im Netzwerkmitschnitt finden: Wireshark richtig einsetzen.

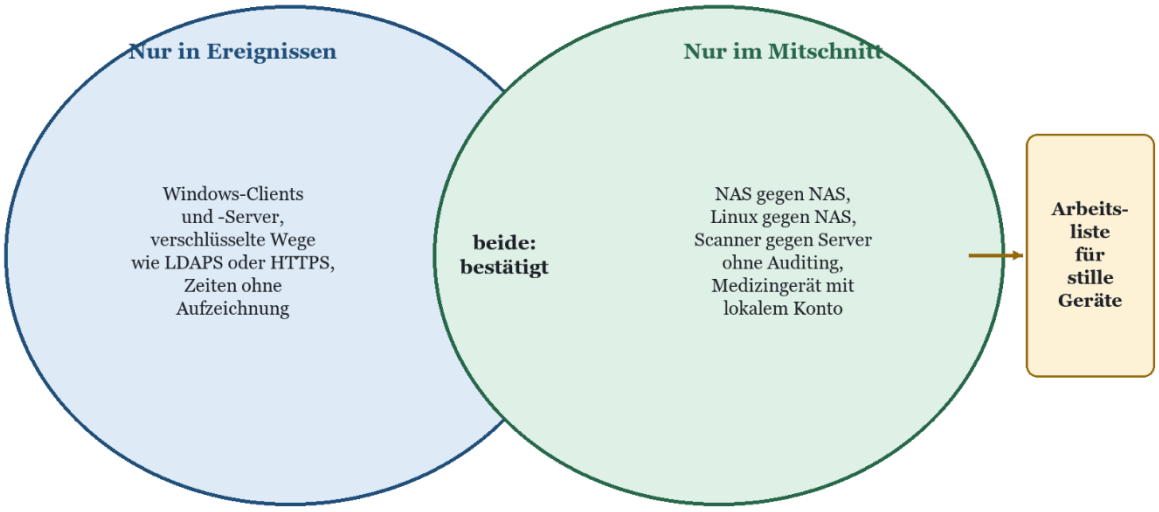
Fundort	Bordmittel	Was du siehst	Was fehlt
Serversicht	4022/4023, 8002, 4624, Get-WinEvent, wevtutil	Konto, Client IP, NTLM-Version, Status	Reason ID, Ursache am Gerät, Gerät gegen Gerät
DC-Sicht	4030 bis 4033, 8004, 4776	Domänenkonto und Arbeitsstation zentral	lokale Konten, Zielsystem teils unklar
Clientsicht	4020/4021 auf Windows-Clients	Ziel (Gerät) und Reason ID	nur wenn Windows der Anrufer ist
Mitschnitt	Wireshark, pktmon	jede unverschlüsselte NTLM-Aushandlung	TLS-Verbindungen, Zeiten ohne Aufzeichnung

Wo es mit Bordmitteln mühsam wird

Jeder Fundort für sich ist beherrschbar. Mühsam wird es beim Zusammenlegen. Die Serversicht liegt auf 40 Dateiservern verteilt, die DC-Sicht auf vier Domain Controllern, der Mitschnitt als Datei mit ein paar Gigabyte auf dem Laptop eines Kollegen. Um herauszufinden, welche Verbindungen nur im Mitschnitt auftauchen, musst du die Treffer aus Wireshark exportieren, nach Quelle, Ziel und Konto normalisieren und gegen Hunderttausende Ereignisse abgleichen. Das ist eine Excel-Übung, bei der man nach dem dritten SVERWEIS beginnt, mit dem Multifunktionsgerät zu sprechen. Und solange du nicht weißt, welche Server überhaupt Ereignisse liefern, kannst du nicht unterscheiden, ob ein Gerät nur im Mitschnitt steht, weil es Gerät gegen Gerät spricht, oder weil der Zielserver schlicht kein Auditing hat.

Ereignisse gegen Mitschnitt: die interessante Menge ist rechts

Was beide Quellen kennen, ist bekannt. Was nur der Mitschnitt kennt, ist dein blinder Fleck.



Skizze: Prinzip des Abgleichs, Inhalte beispielhaft

TIPP · Aufzeichnen, wo die Geräte hinwollen

Zeichne nicht am Rand des Netzes auf, sondern dort, wo die stillen Geräte ihre Daten abliefern: am Dateiserver für Scan to Folder, vor dem NAS für Sicherungen, am Archivserver für die Medizintechnik. Nimm mindestens einen vollen Arbeitstag mit Nachtlauf auf, besser eine Woche mit Monatsende. Manche Geräte melden sich nur einmal im Monat, und zwar genau dann, wenn niemand hinschaut.

Ereignisse und Mitschnitt in einer Sicht

Genau diesen Abgleich übernimmt der NTLM Diagnostiker. Er liest die Ereignisse direkt von den Domain Controllern, aus einem vorhandenen Windows Event Collector oder per Direktabfrage einzelner Rechner, und er liest zusätzlich Netzwerkmitschnitte im pcap- und pcapng-Format ein. Dafür nutzt er tshark aus einer vorhandenen Wireshark-Installation und filtert die NTLMSSP-Anmeldungen aus SMB, HTTP, LDAP und RPC heraus. Die Treffer landen in derselben Kommunikationsmatrix wie die Ereignisse, gekennzeichnet als Quelle „Mitschnitt“.

Für stille Geräte ist die Liste der Verbindungen besonders aufschlussreich, die nur im Mitschnitt auftauchen. Das sind genau die Geräte und Konten, die in keinem Ereignisprotokoll stehen: das NAS, das auf ein zweites NAS repliziert, der Scanner, der auf einen Server ohne Auditing ablegt, das Medizingerät mit lokalem Konto. Spricht ein Gerät im Mitschnitt NTLMv1, landet es direkt auf

der NTLMv1-Hitliste. Der Abdeckungsmonitor und die OS-Landkarte zeigen daneben, welche Windows-Server Ereignisse liefern und welche schweigen, sodass du einen Eintrag in der Liste „nur im Mitschnitt“ richtig einordnen kannst.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Stille Geräte mit Wireshark-Import aufspüren

Mitschnitt einlesen: pcap oder pcapng, ausgewertet mit tshark aus deiner vorhandenen Wireshark-Installation. NTLMSSP-Anmeldungen aus SMB, HTTP, LDAP und RPC werden herausgefiltert.

Eine Matrix für alles: Treffer aus dem Mitschnitt stehen in derselben Kommunikationsmatrix wie die Ereignisse, gekennzeichnet als Quelle „Mitschnitt“. Die Konten-Sicht zeigt, welches Konto dahinter steckt.

Liste „nur im Mitschnitt“: Verbindungen, die in keinem Ereignisprotokoll auftauchen. Das ist deine Arbeitsliste für NAS, Multifunktionsgeräte, Scanner, Linux und Medizintechnik.

NTLMv1 im Mitschnitt: wird erkannt und direkt auf die NTLMv1-Hitliste gesetzt. Sicherheitsflaggen markieren weitere Auffälligkeiten.

Einordnen: Abdeckungsmonitor und OS-Landkarte zeigen, welche Server liefern. Die Ursachen-Engine mit SPN- und DNS-Prüfung bewertet die Windows-Seite, die Abschalt-Simulation zeigt, was eine Sperre treffen würde, die Readiness-Ampel fasst den Stand zusammen.

Datensparsam und ausschließlich lesend: Der Diagnostiker übernimmt nur die NTLM-Metadaten, die Mitschnittdatei selbst wird nicht gespeichert. Er ändert nichts an Servern, Geräten oder Richtlinien.

Ergebnis: Word-Bericht für die IT-Leitung, Excel- oder CSV-Export als Geräteliste für das Team.

Editionen: Express ist kostenlos und liefert den Fünf-Minuten-Befund, die Vollversion testest du 7 Tage, lizenziert wird pro aktivem Computerkonto. Ein Anwendungskatalog, ein Ausnahmelisten- und Skript-Generator, ein Phasenplan, ein Kerberos-Gegencheck und ein Verlauf sind geplant, aber noch nicht enthalten.

› NTLM Diagnostiker

Aufgabe	Mit Bordmitteln	Mit dem NTLM Diagnostiker
Mitschnitt auswerten	Wireshark, Filter ntlmssp, Export von Hand	Wireshark-Import per tshark
Mitschnitt mit Ereignissen abgleichen	Export, Normalisieren, Excel	gemeinsame Kommunikationsmatrix, Quelle „Mitschnitt“
Geräte ohne Ereignisse auflisten	Differenz selbst bilden	Liste „nur im Mitschnitt“
NTLMv1 bei Geräten	Filter auf fehlende NTLMv2-Antwort	NTLMv1-Hitliste
Server ohne Auditing erkennen	Serverliste gegen Ereignisse abgleichen	Abdeckungsmonitor und OS-Landkarte
Eingriff in die Umgebung	je nach Skript	keiner, ausschließlich lesend

AUS DER PRAXIS · Sparfuchs & Partner Steuerberatungs GmbH

Rund 70 Arbeitsplätze, Domäne sparfuchs.local, zwei Dateiserver, ein NAS für Sicherungen, vier Multifunktionsgeräte. Die Ereignisauswertung über drei Wochen sah erfreulich aus: wenige hundert NTLM-Anmeldungen am Tag, fast alle von einem Fachprogramm. Der Mitschnitt vor dem NAS erzählte eine andere Geschichte. Das NAS replizierte nachts per SMB mit einem lokalen Konto auf ein zweites NAS in der Außenstelle, mit NTLMv1. Kein Windows-System war beteiligt, kein Ereignis

existierte.

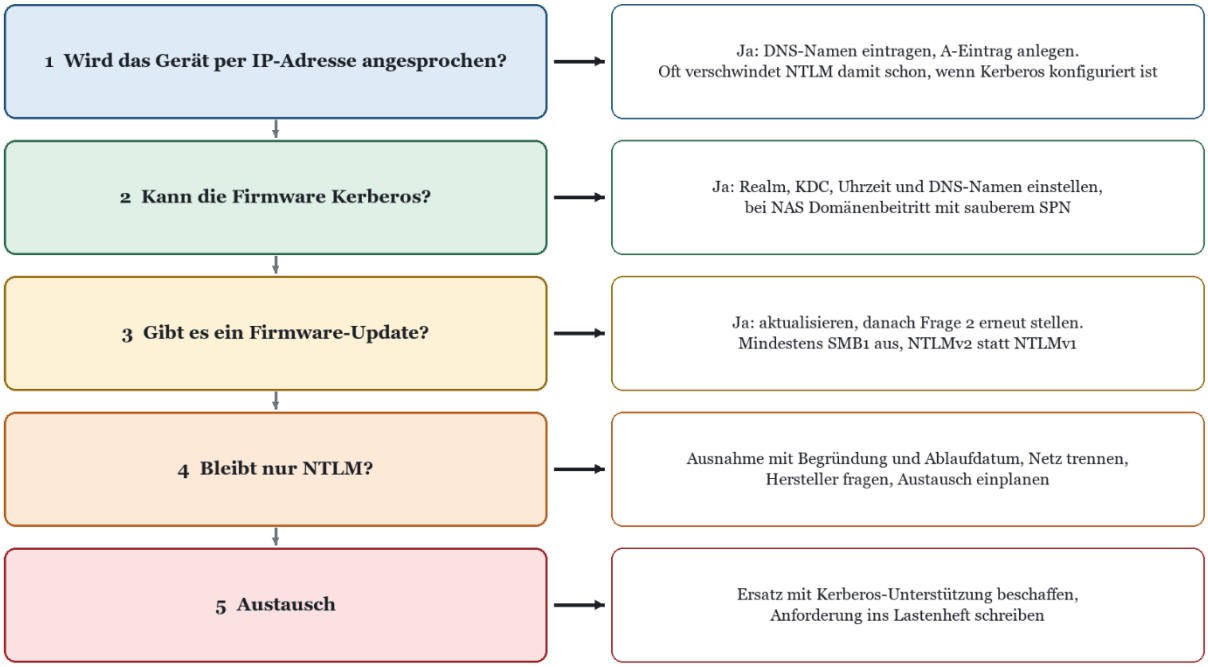
Platz zwei auf der Liste „nur im Mitschnitt“: ein Multifunktionsgerät, das auf einen alten Dateiserver ohne erweitertes Auditing scannte, per IP-Adresse. Firmware-Update, Kerberos im Webinterface eingetragen, Ziel auf den DNS-Namen umgestellt, und das Gerät meldete sich am nächsten Morgen mit Kerberos an. Das NAS-Paar bekam ein Firmware-Update, eine Domänenmitgliedschaft und einen Termin im Beschaffungsplan.

Typische Lösungen: Firmware, Kerberos, SMB, Austausch

Gefunden ist noch nicht gelöst. Die gute Nachricht: Bei stillen Geräten sind die Lösungen überschaubar und wiederholen sich. Die schlechte: Sie liegen meist in einem Webinterface, dessen Administrator-Kennwort auf einem Aufkleber an der Rückseite steht, den jemand 2019 überklebt hat.

Vom Fund zur Lösung: vier Fragen pro Gerät

Von oben nach unten. Austausch ist die letzte Antwort, nicht die erste.



Skizze: eigenes Vorgehensmodell

Firmware aktualisieren

Der erste Blick gilt immer der Firmware. Viele Hersteller haben in den letzten Jahren Kerberos-Unterstützung für SMB nachgerüstet, SMB1 entfernt und NTLMv1 abgeschaltet. Ein Gerät, das heute NTLMv1 spricht, tut das nicht selten nur, weil seine Firmware den Stand der Auslieferung hat. Prüfe vor dem Update die Versionshinweise auf die Stichworte Kerberos, SMB2 oder SMB3 und NTLMv2, und plane bei Medizintechnik immer mit dem Hersteller, nie an ihm vorbei.

Kerberos am Gerät konfigurieren

Kann das Gerät Kerberos, braucht es im Wesentlichen vier Dinge: den Realm in Großbuchstaben, also MUSTERWERK.LOCAL, einen erreichbaren KDC, eine Uhrzeit, die nicht weiter als die erlaubte Toleranz vom Domain Controller abweicht, standardmäßig fünf Minuten, und ein Ziel, das unter seinem DNS-Namen angesprochen wird. Für ein NAS kommt der Domänenbeitritt hinzu, damit es ein Computerkonto mit SPN bekommt. Ob der SPN stimmt, prüfst du mit setspn:

```
setspn -L NAS01                                    # SPNs am Computerkonto des NAS
setspn -Q cifs/nas01.musterwerk.local              # An welchem Konto hängt der SPN?
setspn -Q cifs/archiv.musterwerk.local             # DNS-Alias ohne SPN? Dann NTLM
Resolve-DnsName nas01.musterwerk.local             # A-Eintrag vorhanden?
w32tm /stripchart /computer:10.20.5.31 /samples:3 # Zeitabweichung des Geräts (falls NTP-fähig)
```

Wird das NAS unter einem Alias angesprochen, braucht dieser Alias einen eigenen SPN am Computerkonto des NAS, oder du stellst die Zugriffe auf den eigentlichen Namen um. Beim Scan to Folder trägst du im Webinterface statt der IP-Adresse den vollständigen DNS-Namen des Servers ein. Die Grundlagen zu Tickets, SPNs und Zeittoleranz findest du im Kompetenzbereich Microsoft Kerberos.

SMB-Einstellungen nachziehen

SMB1 gehört abgeschaltet, auf den Geräten wie auf den Servern. Wer SMB1 noch braucht, braucht meist auch NTLMv1, und beides zusammen ist kein Protokoll, sondern eine Einladung. Auf der Windows-Seite fordern aktuelle Versionen wie Windows 11 24H2 und Windows Server 2025 die SMB-Signatur deutlich strenger an als frühere Versionen; alte Geräte scheitern daran gelegentlich schon heute, und zwar nicht an NTLM, sondern an der Signatur. Halte beide Ursachen auseinander, sonst reparierst du das Falsche. Bei Linux stellst du cifs-Einbindungen mit sec=krb5 auf Kerberos um, nachdem das System in der Domäne ist und ein Ticket beziehen kann.

Ausnahme oder Austausch

Manche Geräte können kein Kerberos und werden es nie lernen. Dann bleiben zwei ehrliche Wege. Erstens eine Ausnahme: Mit den Restrict-NTLM-Richtlinien trägst du auf dem Domain Controller Server-Ausnahmen ein, damit ein bestimmter Zielserver weiter NTLM annehmen darf, während der Rest der Domäne gesperrt wird. Jede Ausnahme braucht eine Begründung, einen Verantwortlichen und ein Ablaufdatum, Details in Restrict-NTLM-Richtlinien erklärt: Überwachen, Ausnahmen, Verweigern und Server-Ausnahmen für NTLM: sauber pflegen statt Löcher bohren. Flankierend trennst du das Gerät in ein eigenes Netzsegment und erlaubst nur die Verbindungen, die es braucht. Zweitens der Austausch: Schreib Kerberos-Unterstützung für SMB und LDAP als Muss-Kriterium in jede Ausschreibung, dann erledigt sich das Problem mit dem nächsten Beschaffungszyklus. Was du den Hersteller vorher fragen solltest, steht in Wenn die Anwendung NTLM fest eingebaut hat: Hersteller richtig fragen.

Lösung	Wann sie passt	Aufwand	Risiko
DNS-Namen statt IP	Gerät kann Kerberos, wird aber per IP angesprochen	gering	gering, vorher DNS-Eintrag prüfen
Kerberos konfigurieren	Firmware unterstützt Kerberos	gering bis mittel	Zeit und DNS müssen stimmen
Domänenbeitritt NAS	NAS mit lokalen Konten, Samba-basiert	mittel	Berechtigungen neu vergeben
Firmware-Update	veraltete Firmware, NTLMv1 oder SMB1	mittel	Wartungsfenster, bei Medizintechnik nur mit Hersteller
SMB1 abschalten	Gerät kann SMB2 oder SMB3	gering	Altgeräte vorher identifizieren
Ausnahme mit Netztrennung	kein Kerberos möglich, Austausch noch nicht machbar	mittel	bleibt eine Schwachstelle mit Ablaufdatum
Austausch	kein Update, kein Kerberos, keine Zukunft	hoch	Budget und Lieferzeit

WICHTIG · Erst messen, dann sperren

Bevor du eine Restrict-NTLM-Richtlinie auf Verweigern stellst, muss jedes stille Gerät entweder umgestellt, als Ausnahme dokumentiert oder bewusst abgeschrieben sein. Das gelingt nur mit einem Mitschnitt, der die Geräteseite zeigt. Wer ohne Mitschnitt sperrt, macht den Stichtag zum Test, und die Testergebnisse kommen dann per Telefon.

Die Bewertung von Gerätelisten, Herstellerantworten und Ausnahmen ist ein typischer Punkt, an dem eine zweite Meinung Zeit spart; dafür gibt es die Beratung zur NTLM-Ablösung. Soll dein Team Serversicht, DC-Sicht und Mitschnitt künftig selbst auswerten, ist die Schulung zum NTLM Diagnostiker der kürzere Weg.

FAQ: stille Geräte und NTLM

Warum taucht mein NAS nicht im NTLM-Audit auf?

Weil das erweiterte NTLM-Auditing nur auf Windows-Systemen läuft. Das NAS schreibt keine Windows-Ereignisse. Sichtbar wird es nur über die Gegenseite: auf Windows-Clients, die es ansprechen (4020), auf Windows-Servern, bei denen es sich anmeldet (4022/4023), oder im Mitschnitt.

Kann ein NAS überhaupt Kerberos?

Viele Samba-basierte NAS-Systeme können es, wenn sie Mitglied der Domäne sind, ein Computerkonto mit passenden SPNs besitzen und unter ihrem DNS-Namen angesprochen werden. Zugriffe per IP-Adresse oder mit lokalen Konten des NAS laufen weiter über NTLM.

Mein Multifunktionsgerät scannt per SMB. Muss ich mir Sorgen machen?

Wenn es NTLM verwendet, ja, spätestens mit Phase 3. Prüfe, ob die Firmware Kerberos für Scan to Folder unterstützt, trage Realm, KDC und den DNS-Namen des Ziels ein und kontrolliere die Uhrzeit. Ältere Geräte mit NTLMv1 oder SMB1 brauchen ein Firmware-Update oder einen Nachfolger.

Warum steht in Ereignis 4022 kein Grund für NTLM?

Die Reason ID erscheint nur in der Clientsicht 4020/4021, also wenn ein Windows-System der Anrufer ist. Meldet sich ein Gerät am Server an, kennt Windows den Grund nicht; ihn findest du nur in der Konfiguration des Geräts.

Reicht die DC-Sicht nicht aus?

Für Domänenkonten ist sie ein guter zentraler Fundort. Lokale Konten auf dem Zielserver oder dem NAS und Verbindungen zwischen zwei Nicht-Windows-Geräten erscheinen dort aber nie. Diese Lücke schließt nur der Mitschnitt.

Wo zeichne ich am besten auf?

Dort, wo die Geräte ihre Daten abliefern: am Dateiserver, vor dem NAS, am Archivserver. Auf Windows-Servern genügt pktmon mit anschließender Umwandlung nach pcapng. Zeichne mindestens einen Arbeitstag mit Nachtlauf auf.

Sieht ein Mitschnitt alle NTLM-Anmeldungen?

Nein. Verschlüsselte Verbindungen wie HTTPS, LDAPS oder RDP mit TLS kann kein Mitschnitt einsehen. Für SMB, unverschlüsseltes HTTP, LDAP und RPC funktioniert er gut.

Was macht der NTLM Diagnostiker mit meinem Mitschnitt?

Er liest ihn mit tshark aus deiner Wireshark-Installation, übernimmt nur die NTLM-Metadaten und speichert die Mitschnittdatei nicht. Die Treffer erscheinen als Quelle „Mitschnitt“ in der

Kommunikationsmatrix, Verbindungen ohne Gegenstück im Ereignisprotokoll in der Liste „nur im Mitschnitt“. Er arbeitet ausschließlich lesend.

Fazit: Wer schweigt, wird trotzdem gehört

NAS, Multifunktionsgeräte, Scanner, Medizintechnik und Linux-Systeme sind bei der NTLM-Ablösung nicht schwieriger als Windows-Systeme. Sie sind nur leiser. Wer sich ausschließlich auf Ereignisprotokolle verlässt, zählt die Geräte, die reden, und übersieht die, die am Stichtag ausfallen. Mit Serversicht, DC-Sicht und einem gezielten Mitschnitt bekommst du sie trotzdem auf die Liste.

Danach ist die Arbeit erstaunlich bodenständig: DNS-Namen statt IP-Adressen, Kerberos im Webinterface, Domänenbeitritt für das NAS, Firmware auf Stand, SMB1 raus. Was dann noch übrig bleibt, bekommt eine Ausnahme mit Ablaufdatum oder einen Platz im Beschaffungsplan. Der Onkel auf der Familienfeier sagt dann zwar immer noch nichts. Aber du weißt wenigstens, wo er sitzt.

WEITERLESEN · Weiter in dieser Serie

› NTLM im Netzwerkmitschnitt finden: Wireshark richtig einsetzen
› Ereignis 4022 und 4023: eingehende NTLM-Anmeldungen auf Servern
› NTLM auf dem Domain Controller: Ereignisse 4030 bis 4033 und 8004
› NTLM wegen IP-Adresse: Laufwerke und Skripte auf DNS-Namen umstellen
› NTLM in der Klinik: Medizintechnik, Labor und Fachanwendungen
› Wenn die Anwendung NTLM fest eingebaut hat: Hersteller richtig fragen
› Server-Ausnahmen für NTLM: sauber pflegen statt Löcher bohren
› NTLM-Nutzung ermitteln: der komplette Leitfaden