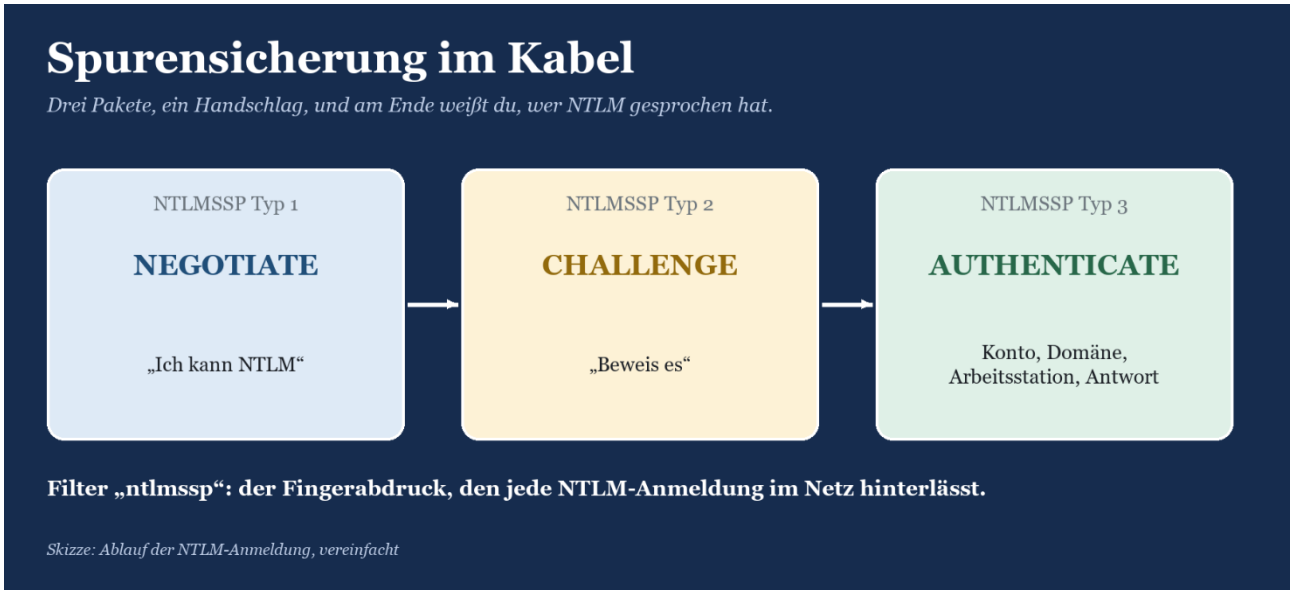
NTLM im Netzwerkmitschnitt finden: Wireshark richtig einsetzen



WISSEN
Wie der NTLM Diagnostiker Mitschnitte über tshark einliest und mit den Ereignissen deiner Domäne zusammenführt.
› **NTLM Diagnostiker**

BERATUNG
Mitschnittpunkte planen, Funde bewerten und stille Geräte in den Ablöseplan aufnehmen.
› **Beratung zur NTLM-Ablösung**

SCHULUNG
Pakete lesen statt raten: NTLMSSP, SPNEGO und Kerberos im Mitschnitt sicher erkennen.
› **Schulung zum NTLM Diagnostiker**

Ereignisprotokolle sind wie Zeugenaussagen: hilfreich, aber nur so gut wie der Zeuge. Ein Windows-Server erzählt dir bereitwillig, wer sich bei ihm per NTLM angemeldet hat. Das NAS im Keller erzählt dir gar nichts, der Scanner im Flur auch nicht, und der Linux-Server, der nachts Sicherungen auf eine Freigabe schiebt, hat eine ausgeprägte Abneigung gegen Windows-Protokolle. Irgendwann kommst du an den Punkt, an dem du nicht mehr den Zeugen glaubst, sondern das Kabel befragst. Dann wird es Zeit für Wireshark.

Wer nach ntlm wireshark sucht, will meist genau eines wissen: Welcher Filter zeigt mir die NTLM-Anmeldungen, und wie erkenne ich, ob da noch NTLMv1 durch die Leitung kriecht? Beides ist schnell erklärt. Schwieriger sind die Fragen davor und danach: Wo schneide ich mit, ohne das halbe Rechenzentrum aufzuzeichnen? Was sehe ich bei verschlüsselten Verbindungen? Und was mache ich mit einer Datei, die im Zweifel mehr über deine Belegschaft verrät als jede Personalakte?

Der Zeitdruck ist dabei real. 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 sich für NTLMv1 konkret geändert hat, steht in NTLMv1 blockiert: was seit Oktober 2026 nicht mehr geht. Hier geht es um das Werkzeug, das auch dort hinsieht, wo kein Ereignisprotokoll mehr hinkommt.

FAKTEN · NTLM im Mitschnitt auf einen Blick

Jede NTLM-Anmeldung besteht aus drei NTLMSSP-Nachrichten: NEGOTIATE (Typ 1), CHALLENGE (Typ 2) und AUTHENTICATE (Typ 3). Konto, Domäne und Arbeitsstation stehen im

Typ 3.

Der Wireshark-Anzeigefilter „ntlmssp“ findet NTLM unabhängig vom Transportprotokoll: in SMB, HTTP, LDAP und DCE/RPC.

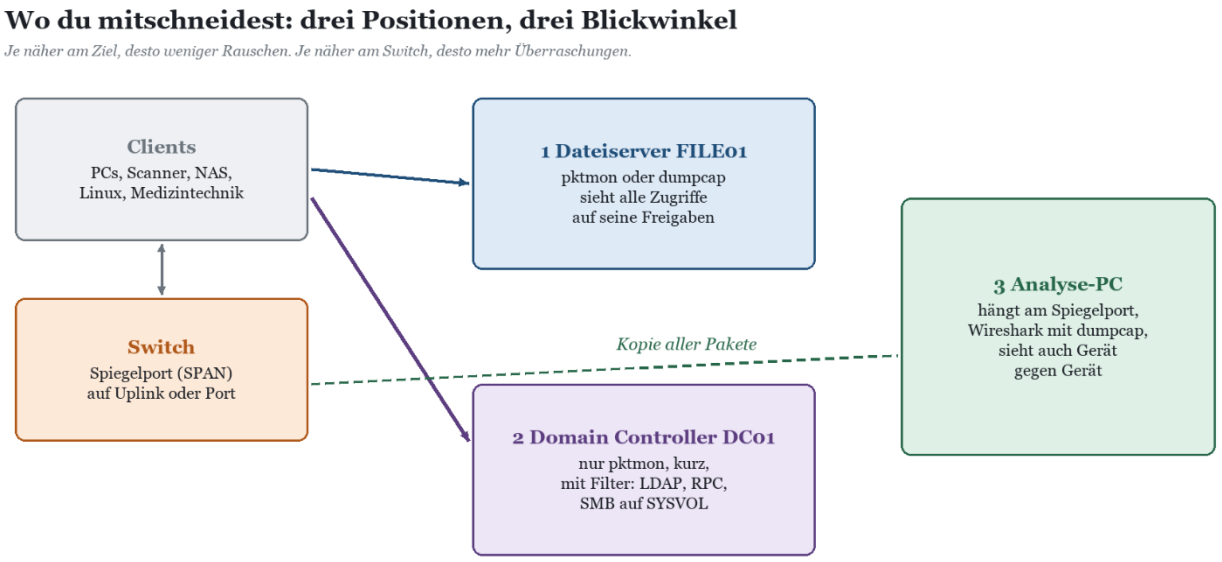
NTLMv1 erkennst du an einer NT-Antwort von genau 24 Bytes ohne den Unterbaum „NTLMv2 Response“.

HTTPS, LDAPS und RDP mit TLS sind im Mitschnitt nicht einsehbar. SMB funktioniert auch bei SMB-Verschlüsselung, weil die Anmeldung vor der Verschlüsselung stattfindet.

Ein Mitschnitt enthält personenbezogene Daten und auswertbares Material für Kennwortangriffe. Werte nur Metadaten aus und bewahre die Datei nicht auf.

Wo du mitschneidest: Dateiserver, DC oder Spiegelport

Der häufigste Anfängerfehler ist nicht der falsche Filter, sondern der falsche Ort. Wer Wireshark auf seinem eigenen Notebook startet, sieht vor allem sein eigenes Notebook. In einem geswitchten Netz bekommst du nur die Pakete, die an dich adressiert sind, plus etwas Broadcast-Gemurmel. Das ist ungefähr so aufschlussreich, wie im eigenen Wohnzimmer nach dem Einbrecher des Nachbarn zu suchen. Für die NTLM-Analyse gibt es drei sinnvolle Positionen.



Faustregel: Dateiserver zuerst, Spiegelport für stille Geräte, DC nur gezielt und kurz.

Skizze: Beispiel Musterwerk GmbH, Namen fiktiv

Position 1: am Dateiserver

Der Dateiserver ist der dankbarste Ort. Hier landen Laufwerkszuordnungen, Scan-to-Folder-Ablagen, Sicherungsjobs und die Skripte, die seit Jahren per IP-Adresse auf \\10.20.1.20\daten zugreifen. Auf einem Windows-Server brauchst du dafür nicht einmal Wireshark: Das Bordmittel pktmon zeichnet Pakete auf und wandelt sie in das pcapng-Format um, das Wireshark und tshark lesen. Wichtig ist der Parameter für die Paketgröße, denn ohne ihn schneidet pktmon jedes Paket nach wenigen Bytes ab, und von der Anmeldung bleibt nur ein abgerissener Zettel.

```
# Aufzeichnung auf FILE01.musterwerk.local, nur SMB
pktmon filter remove
pktmon filter add SMB -t TCP -p 445
pktmon start --capture --pkt-size 0 --file-name C:\Temp\file01.etl --file-size 512 --log-mode
```

```
circular

# ... einen Arbeitstag inklusive Nachtlauf laufen lassen ...
pktmon stop
pktmon etl2pcap C:\Temp\file01.etl --out C:\Temp\file01.pcapng
pktmon filter remove
```

Der Ringpuffer verhindert, dass dir die Aufzeichnung über Nacht die Systemplatte füllt. Plane die Größe so, dass ein voller Arbeitstag hineinpasst. Mit dem Filter auf Port 445 bleibt die Datei erstaunlich klein, solange niemand gerade die Urlaubsfotos der letzten zehn Jahre auf die Freigabe kopiert. Für HTTP-Anwendungen auf demselben Server ergänzt du Port 80 oder den Port der Anwendung.

Position 2: am Domain Controller

Der Domain Controller sieht LDAP-Anmeldungen, RPC-Verbindungen, Zugriffe auf SYSVOL und NETLOGON sowie jede Menge Kerberos. Er ist damit der richtige Ort, wenn du wissen willst, welche Anwendung per LDAP mit NTLM bindet oder welcher Verwaltungsagent per RPC anmeldet. Gleichzeitig ist er der falsche Ort für Experimente. Wireshark samt Paketfiltertreiber hat auf einem DC nichts verloren, pktmon ist dagegen ohnehin an Bord. Zeichne dort kurz, gezielt und mit Filter auf: Port 389 für LDAP, 445 für SMB, 135 für den RPC-Endpunktmapper. Die eigentlichen RPC-Verbindungen laufen über dynamische Ports, deshalb ist für RPC ein Filter auf die IP-Adresse des verdächtigen Clients oft sinnvoller als einer auf Ports.

Eine wichtige Einschränkung: Viele NTLM-Anmeldungen landen am DC gar nicht als NTLMSSP-Paket, sondern als Pass-Through-Prüfung über den sicheren Kanal des Mitgliedsservers. Die eigentliche NTLMSSP-Verhandlung siehst du am Server, bei dem sich der Client anmeldet. Die DC-Sicht dieser Anmeldungen liefern die Ereignisse 8004 und 4030 bis 4033, nicht das Kabel.

Position 3: am Spiegelport

Der Spiegelport, bei manchen Herstellern SPAN-Port oder Port Mirroring genannt, kopiert den Verkehr eines oder mehrerer Switch-Ports auf einen Analyseport. Dort hängt ein Analyse-PC mit Wireshark beziehungsweise dumpcap. Das ist die einzige Position, die auch Verbindungen sieht, an denen kein Windows-System beteiligt ist: NAS gegen NAS, Linux gegen NAS, Medizingerät gegen Archivsystem. Genau diese Verbindungen tauchen in keinem Ereignisprotokoll auf, und genau sie sorgen am Abschalttag für die interessanten Telefonate. Mehr zu diesen Kandidaten steht in NAS, Drucker und Scanner: NTLM bei Geräten ohne Ereignisprotokoll.

```
# Analyse-PC am Spiegelport, Ringpuffer mit 10 Dateien zu je 200 MB
dumpcap -i 2 -f "tcp port 445 or tcp port 80 or tcp port 389 or tcp port 8080" ^
        -b filesize:200000 -b files:10 -w D:\Mitschnitt\span.pcapng
```

Position	Sieht	Sieht nicht	Werkzeug	Eignung
Dateiserver	alle Zugriffe auf seine Freigaben, auch von stillen Geräten	Verkehr zu anderen Servern	pktmon (Bordmittel)	erste Wahl
Domain Controller	LDAP-Binds, RPC, SYSVOL	Pass-Through-Anmeldungen als NTLMSSP	pktmon, kurz und gefiltert	gezielt
Spiegelport	alles auf den gespiegelten Ports, auch Gerät gegen Gerät	andere Switches, verschlüsselte Inhalte	Wireshark oder dumpcap	für stille Geräte
Eigener Client	eigene Verbindungen	fast alles andere	Wireshark	Test einzelner Anwendungen

WARNUNG · Spiegelport ist kein Wunschkonzert

Ein Spiegelport auf einem stark belasteten Uplink verliert Pakete, wenn der Analyseport langsamer ist als die Summe der gespiegelten Ports. Fehlen dir die Hälfte der AUTHENTICATE-Pakete, liegt das nicht an NTLM, sondern an der Physik. Spiegele gezielt die Ports der Ziele, nicht den gesamten Core-Switch, und sprich das Vorhaben mit den Kolleginnen und Kollegen vom Netzwerk ab, bevor du deren Switch-Konfiguration anfasst.

TIPP · Mitschnitt ergänzt das Auditing, ersetzt es nicht

Ein Mitschnitt ist eine Momentaufnahme. Die dauerhafte Sicht liefern die erweiterten NTLM-Ereignisse auf Clients, Servern und DCs. Wie du sie einschaltest, beschreibt Erweitertes NTLM-Auditing einschalten: Schritt für Schritt; die passenden Richtlinien legt das NTLM-Audit-GPO-Skript in einem Durchgang an.

Der Filter ntlmssp und was dahinter steckt

Jetzt der Teil, für den du eigentlich gekommen bist. Öffne die Datei in Wireshark und tippe in die Filterzeile: ntlmssp. Das war es schon. Wireshark zeigt dir alle Pakete, die eine NTLMSSP-Nachricht enthalten, egal in welchem Protokoll sie verpackt ist. Wenn die Liste jetzt leer bleibt, hast du entweder eine vorbildliche Umgebung oder an der falschen Stelle aufgezeichnet. Erfahrungsgemäß ist es das Zweite.

Der Filter „ntlmssp“ ist ein Anzeigefilter, kein Aufzeichnungsfilter. Beim Aufzeichnen mit dumpcap oder pktmon filterst du nach Ports und Adressen; die Auswahl der NTLM-Pakete passiert erst beim Auswerten. Das ist kein Nachteil, denn so kannst du dieselbe Datei auch auf Kerberos prüfen.

Der Dreischritt: NEGOTIATE, CHALLENGE, AUTHENTICATE

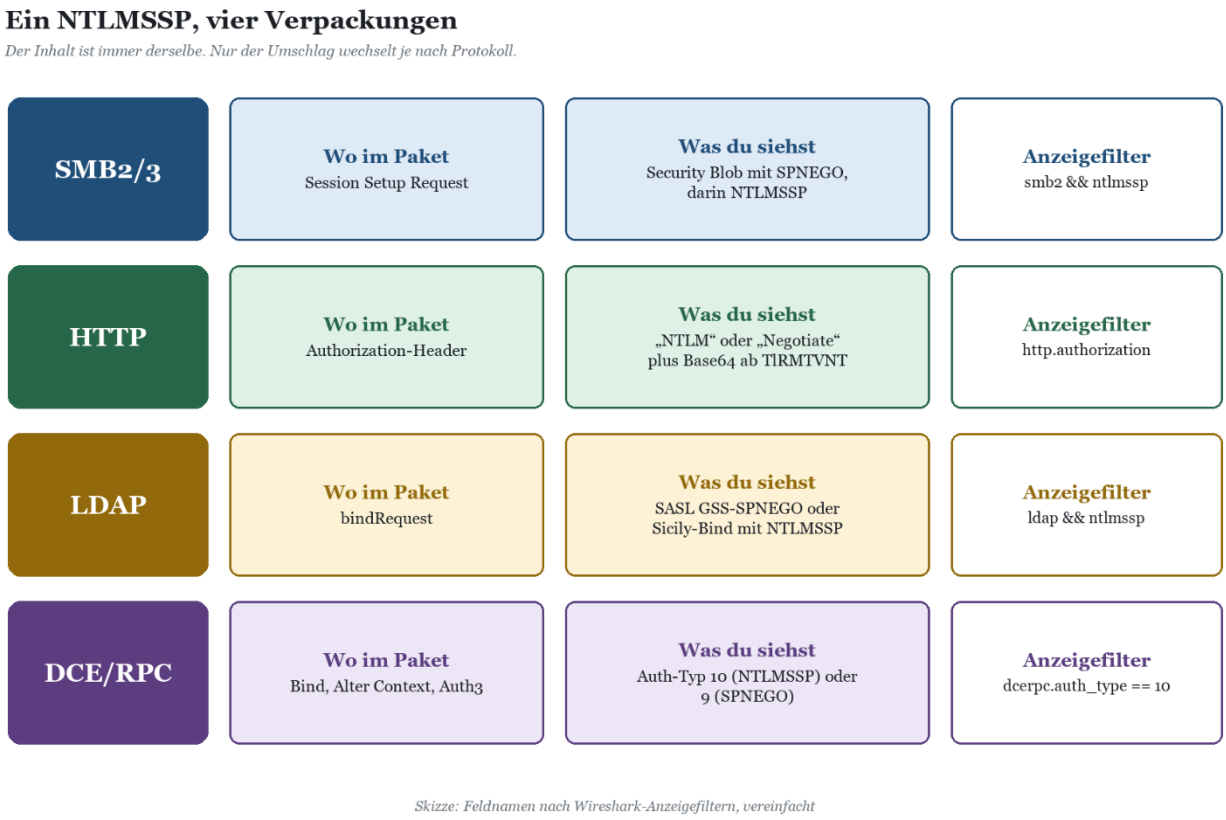
Eine NTLM-Anmeldung besteht immer aus drei Nachrichten. Der Client schickt NEGOTIATE und kündigt an, welche Optionen er beherrscht. Der Server antwortet mit CHALLENGE, einer Zufallszahl und Angaben über sich selbst. Der Client beantwortet die Challenge mit AUTHENTICATE, und darin steht alles, was dich interessiert: Domäne, Benutzername, Name der Arbeitsstation und die kryptografische Antwort. Für eine Bestandsaufnahme reicht deshalb fast immer der Filter auf Typ 3.

Anzeigefilter	Zeigt dir
ntlmssp	alle NTLMSSP-Nachrichten in allen Protokollen
ntlmssp.messagetype == 0x00000003	nur AUTHENTICATE, also eine Zeile pro Anmeldeversuch
ntlmssp.auth.username == "svc_scan"	alle Anmeldungen eines bestimmten Kontos
ntlmssp.auth.hostname	Pakete mit Arbeitsstationsnamen, als Spalte hinzufügen
ntlmssp.ntlmv2_response	Anmeldungen mit NTLMv2-Antwort
ntlmssp.messagetype == 0x00000003 && !ntlmssp.ntlmv2_response	Kandidaten für NTLMv1 (anonyme Anmeldungen aussortieren)
kerberos	Kerberos-Verkehr zum Gegencheck

Ein Rechtsklick auf ein Feld in der Paketdetailansicht und „Als Spalte anwenden“ macht aus Benutzername, Domäne und Arbeitsstation eigene Spalten. Danach sortierst du die Liste und hast in fünf Minuten die erste Hitliste. Für größere Dateien ist tshark auf der Kommandozeile bequemer, weil es das Ergebnis direkt als CSV ausgibt:

```
tshark -r file01.pcapng -Y "ntlmssp.messagetype == 0x00000003" -T fields ^
  -e frame.time -e ip.src -e ip.dst -e tcp.dstport ^
  -e ntlmssp.auth.domain -e ntlmssp.auth.username -e ntlmssp.auth.hostname ^
  -E header=y -E separator=; > ntlm-treffer.csv
```

NTLMSSP in SMB, HTTP, LDAP und RPC



Skizze: Feldnamen nach Wireshark-Anzeigefiltern, vereinfacht

SMB: Beim SMB2- oder SMB3-Session-Setup steckt die Anmeldung im Security Blob, eingepackt in SPNEGO. Wireshark zeigt dir die Liste der angebotenen Verfahren. Steht dort nur NTLMSSP oder wählt der Server NTLMSSP, obwohl Kerberos angeboten wurde, hast du deinen Fund. Ein typischer Grund ist der Zugriff per IP-Adresse, für den kein Kerberos-Ticket existiert; die Umstellung beschreibt NTLM wegen IP-Adresse: Laufwerke und Skripte auf DNS-Namen umstellen.

HTTP: Webanwendungen verhandeln im Header. Der Server schickt „WWW-Authenticate: Negotiate“ oder „WWW-Authenticate: NTLM“, der Client antwortet mit „Authorization:“ und einem Base64-Block. Beginnt dieser mit TlRMTVNT, ist es NTLMSSP, auch wenn davor „Negotiate“ steht. Der Filter http.authorization contains "TlRMTVNT" findet genau diese Fälle. Kerberos-Tickets beginnen dagegen anders und sind deutlich länger. Wie du IIS-Anwendungen auf Negotiate mit Kerberos bringst, steht in NTLM in IIS und Webanwendungen: Negotiate statt NTLM.

LDAP: Anwendungen binden sich per bindRequest an den DC. Mit SASL und GSS-SPNEGO steckt darin entweder Kerberos oder NTLMSSP; ältere Programme nutzen den Microsoft-eigenen Sicily-Bind, der immer NTLM bedeutet. Telefonanlagen, Druckeradressbücher und Fachanwendungen sind hier die üblichen Verdächtigen.

RPC: Bei DCE/RPC steht das Verfahren im Bind-Paket als Authentifizierungstyp. Typ 10 ist NTLMSSP direkt, Typ 9 ist SPNEGO und kann beides enthalten, Typ 16 ist Kerberos. Der Filter

dcerpc.auth_type == 10 zeigt die Programme, die NTLM fest verdrahtet haben. Das sind oft ältere Verwaltungsagenten und Inventarisierungswerkzeuge.

AUS DER PRAXIS · Musterwerk GmbH: der Scanner mit dem langen Gedächtnis

Im Mitschnitt am Dateiserver der fiktiven Musterwerk GmbH tauchten jeden Morgen um kurz nach sieben Uhr NTLM-Anmeldungen des Kontos svc_scan auf, Arbeitsstation leer, Ziel \\10.20.1.20\scan. Die Ereignisse auf dem Server zeigten zwar eingehende NTLM-Anmeldungen, aber keinen Grund. Der Mitschnitt zeigte mehr: eine NT-Antwort von 24 Bytes, also NTLMv1, und SMB-Dialekt 2.0.2. Das Multifunktionsgerät im Lager lief mit einer Firmware von 2016. Nach dem Update und der Umstellung auf den DNS-Namen meldete es sich mit Kerberos an. Ohne Mitschnitt wäre das Gerät erst am Abschalttag aufgefallen, vermutlich mit einem Stapel unscannbarer Lieferscheine als Beweismittel.

NTLMv1 und NTLMv2 im Paket erkennen

Seit dem 13.10.2026 ist NTLMv1 kein theoretisches Risiko mehr, sondern ein praktisches Ausfallrisiko. Ereignis 4024 und 4025 melden dir auf aktuellen Windows-Systemen, wo NTLMv1 für Single Sign-on verwendet oder blockiert wurde; die Details stehen in Ereignis 4024 und 4025: NTLMv1 im Protokoll erkennen. Für Geräte, die keine Ereignisse schreiben, ist der Mitschnitt die einzige Quelle. Die gute Nachricht: Im Paket ist die Unterscheidung eindeutig.



Skizze: Darstellung wie in der Paketdetailansicht von Wireshark, vereinfacht

Die Länge der NT-Antwort

Öffne ein AUTHENTICATE-Paket und klappe den NTLMSSP-Teil auf. Bei NTLMv1 findest du ein Feld „NTLM Response“ mit genau 24 Bytes, sonst nichts. Bei NTLMv2 ist die Antwort deutlich länger, und Wireshark zerlegt sie in einen eigenen Unterbaum „NTLMv2 Response“ mit NTProofStr, Client-Challenge, Zeitstempel und einer Liste von Attributen. Diese Struktur ist das zuverlässigste Unterscheidungsmerkmal, weil sie nicht von Aushandlungsflaggen abhängt, sondern von dem, was tatsächlich gesendet wurde.

Die Falle Extended Session Security

In der NEGOTIATE- und CHALLENGE-Nachricht siehst du eine lange Liste von Flaggen, darunter „Negotiate Extended Session Security“. Diese Variante wurde früher gern als NTLM2 Session Response bezeichnet, was ungefähr so hilfreich ist wie ein Schild „Fast Bio“. Sie verbessert die Sitzungsschlüssel, bleibt aber bei der Anmeldung NTLMv1 mit 24-Byte-Antwort. Lass dich von der Flagge nicht beruhigen: Entscheidend ist die NT-Antwort.

Anonyme Anmeldungen aussortieren

Der Filter auf fehlende NTLMv2-Antworten findet auch anonyme Anmeldungen, bei denen Konto und Antworten leer sind. Die sind für die NTLMv1-Frage uninteressant und gehören in eine eigene Liste. Ergänze den Filter um ntlmssp.auth.username != "" oder sortiere in der CSV nach leeren Benutzernamen. Was übrig bleibt, ist deine NTLMv1-Arbeitsliste.

Merkmal im Paket	NTLMv1	NTLMv2
Länge der NT-Antwort	genau 24 Bytes	deutlich länger, variabel
Unterbaum „NTLMv2 Response“	fehlt	vorhanden
Zeitstempel und Client-Challenge	fehlen	vorhanden
Flagge Extended Session Security	möglich, ändert nichts an v1	üblich
MIC-Feld	fehlt in der Regel	bei aktuellen Clients üblich
Bewertung	dringend ablösen	ablösen bis Phase 3

Das MIC-Feld, der Message Integrity Code, schützt die drei Nachrichten gegen Manipulation und spielt beim Schutz gegen Relay-Angriffe eine wichtige Rolle. Wenn du im Mitschnitt schon dabei bist, lohnt ein Blick darauf; die Hintergründe stehen in NTLM-Relay verhindern: MIC, Kanalbindung und erweiterter Schutz.

WICHTIG · Ein Paket ist kein Urteil

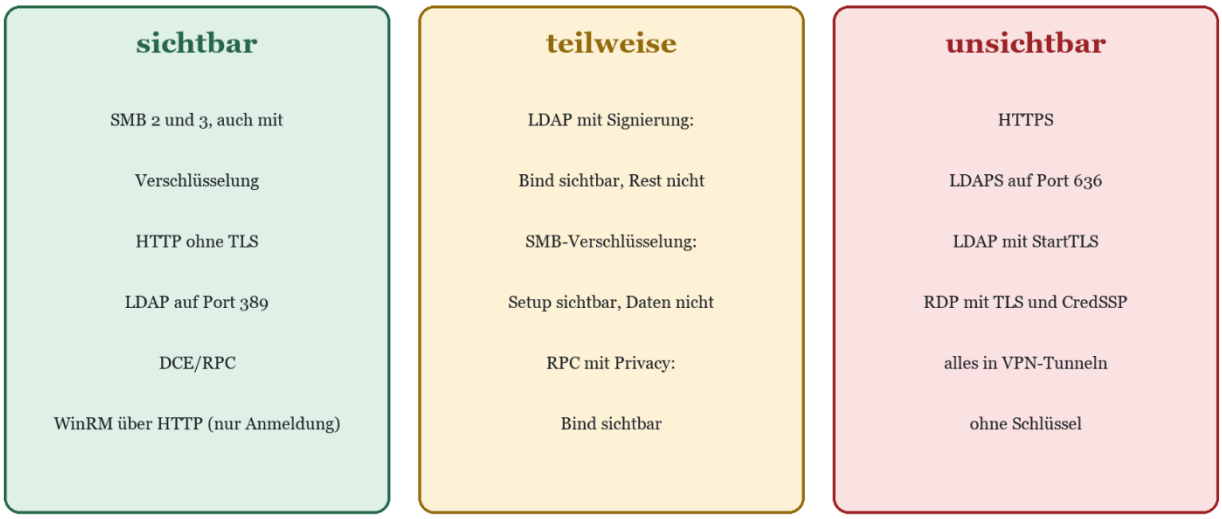
Ein einzelnes NTLMv1-Paket sagt dir, dass ein Gerät NTLMv1 kann und es in diesem Moment benutzt hat. Es sagt dir nicht, ob die Gegenstelle es akzeptiert hat. Prüfe deshalb auch die Antwort des Servers: Bei SMB zeigt der Status der Session-Setup-Antwort, ob die Anmeldung erfolgreich war. Ein abgewiesener Versuch ist ein anderes Problem als ein erfolgreicher.

Grenzen: HTTPS, LDAPS und RDP mit TLS

Wireshark ist kein Röntgengerät. Was in TLS verpackt ist, bleibt verpackt. Das ist sicherheitstechnisch eine gute Nachricht und analytisch eine schlechte. Für die NTLM-Suche heißt das: Je moderner eine Verbindung abgesichert ist, desto weniger siehst du im Mitschnitt, und desto wichtiger werden die Ereignisse auf den Endpunkten.

Was der Mitschnitt sieht und was nicht

Entscheidend ist, ob die Anmeldung vor oder nach dem Verschlüsseln stattfindet.



Skizze: Für die unsichtbaren Fälle bleiben die Ereignisprotokolle der Endpunkte

Bei HTTPS liegt der Authorization-Header innerhalb von TLS. Du siehst die Verbindung, den Servernamen aus dem TLS-Handshake und die Datenmenge, aber nicht, ob darin NTLM oder Kerberos verhandelt wird. LDAPS auf Port 636 und LDAP mit StartTLS verhalten sich genauso. RDP mit Netzwerkebenen-Authentifizierung verpackt die Anmeldung in CredSSP, und das läuft innerhalb von TLS. Dass dein Jump-Server ständig NTLM spricht, erfährst du dort also nicht aus dem Kabel, sondern aus den Ereignissen 4020 und 4021 auf dem Client; mehr dazu in Ereignis 4020 und 4021: ausgehende NTLM-Anmeldungen lesen.

Anders bei SMB: Auch bei SMB-Verschlüsselung findet das Session Setup unverschlüsselt statt, denn die Schlüssel entstehen ja erst aus der Anmeldung. Ähnlich bei LDAP mit Signierung und Versiegelung über SASL: Der Bind ist sichtbar, alles danach nicht. Dasselbe gilt für RPC mit Packet Privacy. Für die NTLM-Bestandsaufnahme reicht das, denn du willst ja die Anmeldung sehen, nicht den Inhalt.

Verbindung	NTLM im Mitschnitt?	Alternative Quelle
SMB 2/3, auch verschlüsselt	ja, im Session Setup	4022/4023 auf dem Server
HTTP ohne TLS	ja, im Authorization-Header	4022/4023, IIS-Protokoll
HTTPS	nein	4020/4021 auf dem Client, 4022/4023 auf dem Server
LDAP 389 mit SASL	ja, im bindRequest	4030 bis 4033 und 8004 am DC
LDAPS 636, StartTLS	nein	Ereignisse am DC
DCE/RPC	ja, im Bind	4020 bis 4023
RDP mit TLS und CredSSP	nein	4020/4021 auf dem Client

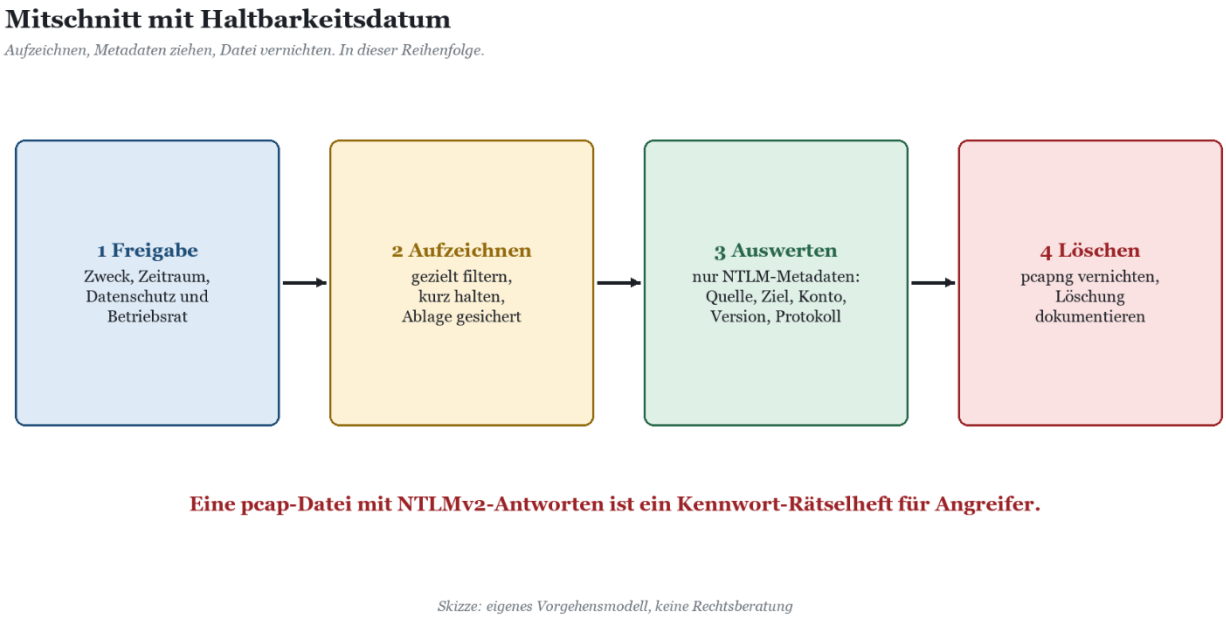
TIPP · TLS-Schlüssel sind keine Abkürzung

Wireshark kann TLS mit vorliegenden Sitzungsschlüsseln entschlüsseln. Für die NTLM-Bestandsaufnahme ist das aber meist ein Umweg: Du müsstest Schlüssel aus Browsern oder Servern exportieren und hättest danach die vollständigen Inhalte im Mitschnitt, also genau das, was du aus

Datenschutzgründen vermeiden willst. Nimm für verschlüsselte Verbindungen die Ereignisse der Endpunkte.

Datenschutz beim Mitschnitt und der Weg in die Auswertung

Ein Netzwerkmitschnitt ist datenschutzrechtlich kein Kavaliersdelikt. Er enthält Benutzernamen, Rechnernamen, IP-Adressen, Dateinamen, bei HTTP auch Inhalte, und er erlaubt Rückschlüsse darauf, wer wann was gemacht hat. Damit ist er ein Fall für Zweckbindung, Datensparsamkeit und, je nach Organisation, für den Betriebsrat oder den Personalrat. Das gilt in der Klinik noch einmal verschärft, wo zwischen Paketen gern auch Patientendaten unterwegs sind; dazu passt NTLM in der Klinik: Medizintechnik, Labor und Fachanwendungen.



Nur Metadaten auswerten

Für die NTLM-Ablösung brauchst du sehr wenig: Zeitpunkt, Quelle, Ziel, Port, Protokoll, Konto, Domäne, Arbeitsstation und NTLM-Version. Das ist genau die CSV aus dem tshark-Befehl oben. Alles andere, also Dateiinhalte, Webseiten und Abfrageergebnisse, ist für den Zweck unnötig. Begrenze bereits die Aufzeichnung auf die relevanten Ports und Ziele, halte den Zeitraum kurz und schreibe vorher auf, wozu du aufzeichnest. Was du mit Datenschutz und Arbeitnehmervertretung vorab klären solltest, beschreibt NTLM-Audit, Datenschutz und Betriebsrat: was du beachten musst.

Die Datei nicht aufbewahren

Jetzt der schwarzhumorige Teil, der leider keiner ist: Ein Mitschnitt mit NTLM-Anmeldungen enthält Challenge und Antwort jeder Anmeldung. Mit diesen Daten lassen sich Kennwörter offline angreifen, bei NTLMv1 erschreckend schnell, bei NTLMv2 und schwachen Kennwörtern immer noch lästig schnell. Eine pcapng-Datei auf dem Desktop des Administrators ist damit ein Geschenkkorb für jeden, der nach einem Einbruch in Ruhe stöbert. Ziehe die Metadaten heraus, lösche die Datei und dokumentiere die Löschung. Archiviert wird die Auswertung, nicht der Mitschnitt.

WARNUNG · Kein Mitschnitt im Ticketsystem

Der Klassiker: Jemand hängt die pcapng-Datei an das Ticket für den Hersteller, das Ticket wird exportiert, archiviert, gesichert und repliziert. Ab diesem Moment liegen die Anmeldedaten deiner

Belegschaft an Orten, die niemand mehr überblickt. Schicke Herstellern gefilterte Auszüge, keine Rohdaten.

Wo es mit Bordmitteln mühsam wird

Bis hierhin kommst du mit pktmon, Wireshark und tshark gut zurecht. Ein Mitschnitt, ein Filter, eine CSV, fertig. In echten Umgebungen bleibt es aber selten bei einem Mitschnitt. Die Sparfuchs & Partner Steuerberatungs GmbH hat einen Dateiserver und ein NAS, das ist an einem Nachmittag erledigt. Die Musterwerk GmbH hat drei Standorte, zwei Dateiserver pro Standort, einen Spiegelport im Rechenzentrum und mehrere Hundert Clients. Dann liegen plötzlich zwölf CSV-Dateien nebeneinander, und die eigentliche Arbeit beginnt erst: Welche dieser Verbindungen kenne ich schon aus den Ereignissen? Welche tauchen nur im Mitschnitt auf? Welcher Rechner gehört zu welcher IP-Adresse? Und warum hat der Client überhaupt NTLM genommen?

Diese Zusammenführung ist der Punkt, an dem Excel-Tabellen anfangen, ein Eigenleben zu entwickeln. Der NTLM Diagnostiker nimmt dir genau diesen Teil ab: Er liest den Mitschnitt ein, legt die Treffer neben die Ereignisse deiner Domäne und zeigt dir die Verbindungen, die nur im Kabel sichtbar sind. Einen Vergleich der Wege mit Bordmitteln, Skripten und Diagnostiker findest du in NTLM-Analyse im Vergleich: Bordmittel, Skripte und NTLM Diagnostiker.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Mitschnitt einlesen, Metadaten behalten, Datei vergessen

Der NTLM Diagnostiker importiert Mitschnitte im Format pcap und pcapng. Dafür nutzt er tshark aus einer vorhandenen Wireshark-Installation und filtert NTLMSSP-Anmeldungen aus SMB, HTTP, LDAP und RPC heraus.

Übernommen werden nur die NTLM-Metadaten. Die Mitschnittdatei selbst speichert er weder als Kopie noch in seiner Datenbank. Wie im übrigen Betrieb arbeitet er dabei ausschließlich lesend: Er ändert keine Gruppenrichtlinien, keine Registrierungswerte und keine Konten.

Die Treffer erscheinen in derselben Kommunikationsmatrix wie die Ereignisse, markiert mit der Quelle „Mitschnitt“. Besonders aufschlussreich sind Verbindungen, die nur im Mitschnitt auftauchen: NAS, Drucker, Scanner, Linux-Server und Medizintechnik.

NTLMv1 erkennt er auch im Mitschnitt und setzt die Funde auf die NTLMv1-Hitliste. Für die Ereignisseite stehen die Ursachen-Engine mit SPN- und DNS-Prüfung, die Konten-Sicht, die Abschalt-Simulation sowie Word-Bericht und Excel/CSV-Export bereit.

Der Wireshark-Import gehört zum vollen Funktionsumfang, den du im siebentägigen Testzeitraum kostenlos ausprobieren kannst. Die kostenlose Edition Express liefert vorab einen Fünf-Minuten-Befund mit Readiness-Ampel direkt aus den Ereignissen der Domain Controller. Lizenziert wird pro aktivem Computerkonto.

Bei der Trendforge Digital GmbH sah das so aus: Ein Tag Mitschnitt am Dateiserver, Import in den Diagnostiker, und von 41 Verbindungen mit NTLM waren 33 schon aus den Ereignissen bekannt. Die übrigen acht waren zwei Linux-Sicherungsjobs, ein NAS mit Replikation und fünf Entwicklungsrechner mit einem alten Build-Werkzeug. Das sind acht Zeilen, die vorher in keiner Liste standen, und genau die acht, die beim Abschalten Ärger gemacht hätten.

Wenn du Mitschnittpunkte, Zeitfenster und Datenschutzfragen nicht allein planen möchtest, unterstützt dich die Beratung zur NTLM-Ablösung. Wer im Team künftig selbst Pakete lesen und Funde sicher bewerten will, ist in der Schulung zum NTLM Diagnostiker richtig.

FAQ: NTLM und Wireshark

Mit welchem Filter finde ich NTLM in Wireshark?

Mit dem Anzeigefilter ntlmssp. Für eine Zeile pro Anmeldeversuch nimmst du ntlmssp.messagetype == 0x00000003, also nur die AUTHENTICATE-Nachrichten.

Wie erkenne ich NTLMv1 im Mitschnitt?

An einer NT-Antwort von genau 24 Bytes im AUTHENTICATE-Paket und am fehlenden Unterbaum „NTLMv2 Response“. Die Flagge Extended Session Security ändert daran nichts. Anonyme Anmeldungen mit leerem Konto sortierst du vorher aus.

Darf ich Wireshark auf dem Domain Controller installieren?

Technisch geht es, empfehlenswert ist es nicht. Auf dem DC nimmst du besser das Bordmittel pktmon, zeichnest kurz und gefiltert auf und wertest die umgewandelte pcapng-Datei auf einem Analyse-PC aus.

Warum sehe ich am DC kaum NTLMSSP-Pakete, obwohl die Ereignisse viel NTLM zeigen?

Weil die meisten NTLM-Anmeldungen an Mitgliedsservern stattfinden und der Server die Prüfung über seinen sicheren Kanal an den DC weiterreicht. Die NTLMSSP-Verhandlung siehst du am Mitgliedsserver, die DC-Sicht in den Ereignissen 8004 und 4030 bis 4033.

Sehe ich NTLM auch bei verschlüsseltem SMB?

Ja. Das Session Setup und damit die Anmeldung laufen vor der Verschlüsselung. Nur die Dateiinhalte danach sind verschlüsselt.

Und bei HTTPS, LDAPS oder RDP?

Nein. Dort steckt die Anmeldung innerhalb von TLS. Für diese Verbindungen nutzt du die Ereignisse 4020/4021 auf dem Client und 4022/4023 auf dem Server.

Wie lange sollte ich mitschneiden?

Mindestens einen vollen Arbeitstag inklusive Nachtlauf, besser zusätzlich einen Monatswechsel, wenn dort Abrechnungs- oder Sicherungsjobs laufen. Mit Port-Filtern und Ringpuffer bleibt die Datei beherrschbar.

Was mache ich mit der pcapng-Datei nach der Auswertung?

Löschen und die Löschung dokumentieren. Die Datei enthält Challenge und Antwort jeder Anmeldung und damit Material für Kennwortangriffe. Aufbewahrt wird nur die Auswertung mit den Metadaten.

Was übernimmt der NTLM Diagnostiker aus meinem Mitschnitt?

Nur die NTLM-Metadaten. Er liest die Datei über tshark aus einer vorhandenen Wireshark-Installation, speichert sie selbst aber weder als Kopie noch in der Datenbank und arbeitet ausschließlich lesend.

Fazit: Das Kabel lügt nicht, es schweigt nur manchmal

Wireshark ist bei der NTLM-Ablösung kein Ersatz für das Auditing, sondern sein Kronzeuge für die Fälle, in denen niemand sonst aussagt. Mit dem richtigen Ort, dem Filter ntlmssp und einem Blick auf die Länge der NT-Antwort findest du stille Geräte, NTLMv1-Altlasten und fest verdrahtete Anwendungen, die in keinem Ereignisprotokoll auftauchen. Wo TLS im Spiel ist, übernehmen wieder die Ereignisse der Endpunkte.

Behandle den Mitschnitt dabei wie das, was er ist: ein Beweisstück mit Verfallsdatum. Gezielt aufzeichnen, Metadaten ziehen, Datei vernichten. Dann bleibt am Ende eine saubere Liste, und keine Datei, die dir nach dem nächsten Sicherheitsvorfall um die Ohren fliegt. Und wenn die Liste länger wird als dein Feierabend, weißt du ja jetzt, wer dir beim Zusammenführen hilft. Für die Kerberos-Seite der Medaille lohnt sich ein Blick auf Microsoft Kerberos.

WEITERLESEN · Weiter in dieser Serie

› NTLM-Nutzung ermitteln: der komplette Leitfaden
› NAS, Drucker und Scanner: NTLM bei Geräten ohne Ereignisprotokoll
› Ereignis 4024 und 4025: NTLMv1 im Protokoll erkennen
› Ereignis 4022 und 4023: eingehende NTLM-Anmeldungen auf Servern
› NTLM in IIS und Webanwendungen: Negotiate statt NTLM
› NTLM-Relay verhindern: MIC, Kanalbindung und erweiterter Schutz
› NTLM-Audit, Datenschutz und Betriebsrat: was du beachten musst
› NTLM-Analyse im Vergleich: Bordmittel, Skripte und NTLM Diagnostiker