Wie sollte die NTLM-Authentifizierung auf Paketebene aussehen?

Inhalt

Einführung

Dieses Dokument beschreibt die NT LAN Manager (NTLM) Authentifizierung auf Paketebene.

Wie sollte die NTLM-Authentifizierung auf Paketebene aussehen?

Eine Paketerfassung nach diesem Artikel kann hier heruntergeladen werden: https://supportforums.cisco.com/sites/default/files/attachments/document/ntlm_auth.zip

Client-IP: 10.122.142.190

WSA-IP: 10.122.144.182

Paketnummer und Details

4. Der Client sendet eine GET-Anforderung an den Proxy.

#7 Der Proxy sendet eine 407 zurück. Das bedeutet, dass der Proxy Datenverkehr aufgrund fehlender ordnungsgemäßer Authentifizierung nicht zulässt. Wenn Sie sich die HTTP-Header in dieser Antwort anschauen, sehen Sie eine "Proxy-Authentication: NTLM". Dies weist den Client darauf hin, dass NTLM eine akzeptable Authentifizierungsmethode ist. Genauso, wenn der Header "Proxy-Authenticate: Basic" vorhanden ist, teilt der Proxy dem Client mit, dass grundlegende Anmeldeinformationen zulässig sind. Wenn beide Header vorhanden sind (häufig), entscheidet der Client, welche Authentifizierungsmethode er verwendet.

Beachten Sie, dass der Authentifizierungs-Header "Proxy-authentication:" lautet. Dies liegt daran, dass die Verbindung in der Erfassung expliziten Weiterleitungsproxy verwendet. Wenn es sich um eine transparente Proxy-Bereitstellung handelt, wäre der Antwortcode 401 anstatt 407 und die Header wären "www-authentication:" statt "proxy-authentiate:".

#8 Die Proxy-FINs dieses TCP-Socket. Das ist richtig und normal.

#15 Auf einem neuen TCP-Socket führt der Client eine weitere GET-Anforderung durch. Dieses Mal beachten Sie, dass GET den HTTP-Header "proxy-authorized:" enthält. Diese enthält eine codierte Zeichenfolge, die Details zum Benutzer / zur Domäne enthält.

Wenn Sie die Proxy-Autorisierung > NTLMSSP erweitern, werden die decodierten Informationen

in den NTLM-Daten gesendet. Im "NTLM Message Type" (NTLM-Nachrichtentyp) wird "NTLMSSP_NEGOTIATE" (NTLMSSP_NEGOTIATE) angezeigt. Dies ist der erste Schritt im Drei-Wege-NTLM-Handshake.

17 Der Proxy antwortet mit weiteren 407. Ein weiterer "proxy-authentiate"-Header ist vorhanden. Dieses Mal enthält es eine NTLM-Probelesungszeichenfolge. Wenn Sie diese weiter erweitern, sehen Sie den NTLM-Meldungstyp "NTLMSSP_CHALLENGE". Dies ist der zweite Schritt im Drei-Wege-NTLM-Handshake.

Bei der NTLM-Authentifizierung sendet der Windows-Domänen-Controller eine Challenge-Zeichenfolge an den Client. Der Client wendet dann einen Algorithmus auf die NTLM-Herausforderung an, der das Kennwort des Benutzers in den Prozess einbezieht. Auf diese Weise kann der Domänencontroller überprüfen, ob der Client das richtige Kennwort kennt, ohne dass das Kennwort über die Leitung übertragen wird. Dies ist viel sicherer als einfache Anmeldeinformationen, bei denen das Kennwort im Klartext an alle Sniffing-Geräte gesendet wird.

18 Der Kunde sendet eine letzte GET-Datei. Beachten Sie, dass sich diese GET-Verbindung auf demselben TCP-Socket befindet wie die NTLM-Negotiate- und NTLM-Challenge. Dies ist für den NTLM-Prozess unerlässlich. Der gesamte Handshake muss auf demselben TCP-Socket ausgeführt werden, andernfalls ist die Authentifizierung ungültig.

In dieser Anforderung sendet der Client die modifizierte NTLM Challenge (NTLM Response) an den Proxy. Dies ist der letzte Schritt im Drei-Wege-NTLM-Handshake.

21 Der Proxy sendet eine HTTP-Antwort zurück. Das bedeutet, dass der Proxy die Anmeldeinformationen akzeptiert und beschlossen hat, den Inhalt zu liefern.