Hoe zou de NTLM-verificatie er op het pakketniveau moeten uitzien?

Inhoud

Inleiding

Dit document beschrijft de verificatie van NT LAN Manager (NTLM) op het pakketniveau.

Hoe zou de NTLM-verificatie er op het pakketniveau moeten uitzien?

U kunt hier een pakketvastlegging naar dit artikel downloaden op:
https://supportforums.cisco.com/sites/default/files/attachments/document/ntlm_auth.zip

IP-client: 10.122.142.190

WSA IP: 10.122.144.182

Packet-nummer en -gegevens

#4 De klant stuurt een GET aanvraag naar de proxy.

#7 De proxy stuurt een 407 terug. Dit betekent dat de proxy geen verkeer toestaat vanwege een gebrek aan juiste authenticatie. Als je naar de HTTP headers in deze reactie kijkt, zie je een "Proxy-echt": NTLM". Dit vertelt de cliënt dat een aanvaardbare methode van authenticatie NTLM is. Als de kop "Proxy-echt" op dezelfde manier wordt gedraaid: Basic" is erbij, zegt de proxy tegen de client dat basisaanmeldingsgegevens acceptabel zijn. Als beide headers aanwezig zijn (common), beslist de client welke methode van authenticatie het zal gebruiken.

Een ding om op te merken is dat de authenticatieheader "Proxy-echt:" is. Dit komt doordat de verbinding in opname expliciete voorwaartse volmacht gebruikt. Als dit een transparante proxy-implementatie was, zou de responscode 401 in plaats van 407 zijn en zouden de headers "www-echt-hebben:" in plaats van "proxy-echt:".

#8 De proxy FIN's is dit TCP socket. Dit is correct en normaal.

#15 In een nieuw TCP socket voert de client een ander GET aanvraag uit. Dit keer merk je op dat de GET de HTTP header "proxy-approval:" bevat. Dit bevat een gecodeerde string die details bevat over de User / Domain.

Als u de Proxy-autorisatie > NTLMSSP uitbreidt, ziet u de gedecodeerde informatie die in de NTLM gegevens wordt verzonden. In het "NTLM Message Type", merkt u op dat het

"NTLMSSP_NEGOTIATE" is. Dit is de eerste stap in de drievoudige NTLM-handdruk.

#17 De proxy reageert met nog eens 407. Er staat een header die "proxy-echt" is. Deze keer bevat het een NTLM challenge string. Als u het nog verder uitbreidt, ziet u dat het NTLM-berichttype "NTLMSSP_CHALLENGE" is. Dit is de tweede stap in de drievoudige NTLM-handdruk.

Bij NTLM-verificatie stuurt de Windows-domeincontroller een challenge-string naar de client. De client past vervolgens een algoritme toe op de NTLM-toets, die factoren in het wachtwoord van de gebruiker tijdens het proces. Hiermee kan de domeincontroller controleren of de client het juiste wachtwoord kent zonder het wachtwoord over de lijn te verzenden. Dit is veel veiliger dan basisgeloofsbrieven, waarin het wachtwoord in gewone tekst wordt verzonden voor alle snipapparaten om te zien.

#18 De klant stuurt een finale. Merk op dat dit GET op hetzelfde TCP stopcontact staat als dat de NTLM-onderhandeling en NTLM-uitdaging optraden. Dit is essentieel voor het NTLM-proces. De gehele handdruk moet op dezelfde TCP socket voorkomen, anders is de verificatie ongeldig.

In dit verzoek stuurt de klant de gewijzigde NTLM Challenge (NTLM Response) naar de proxy. Dit is de laatste stap in de drievoudige NTLM-handdruk.

#21 De proxy stuurt een HTTP-respons. Dit betekent dat de proxy de aanmeldingsgegevens accepteerde en heeft besloten de inhoud op te geven.