Queest-ce que l'authentification NTLM devrait ressembler au niveau de paquet ?

Contenu

Question :

Queest-ce que l'authentification NTLM devrait ressembler au niveau de paquet ?

client ip.addr==165.2.2.129.158
ip.addr==165.202.2.150 WSA>

Nombre/détails de paquet :

#4 le client envoie une demande GET au proxy

#6 le proxy renvoie des 407. Ceci signifie que le proxy ne permet pas le trafic dû à un manque d'authentification appropriée. Si vous regardez les en-têtes de HTTP dans cette réponse, vous verrez « Proxy-pour authentifier : NTLM ». Ceci indique au client qu'une méthode d'authentification acceptable est NTLM. De même, si l'en-tête « Proxy-authentifient : De base » étaient le présent, le proxy serait disant au client que les qualifications de base sont acceptables. Si les deux en-têtes sont présentes (commun), le client décidera quelle méthode d'authentification elle utilisera.

Une chose à noter est que l'en-tête d'authentification est « Proxy-authentifient : ". C'est parce que la connexion dans la capture utilise le proxy en avant explicite. Si c'étaient un déploiement transparent de proxy, le code de réponse serait 401, au lieu de 407, et les en-têtes seraient « WWW-authentifient : » au lieu de « proxy-authentifiez : ".

#8 les FINS de proxy ce socket de TCP. C'est correct et normal.

#15 sur un nouveau socket de TCP le client effectue une autre demande GET. Cet avis de temps que l'OBTENIR proxy-autorisation contient de HTTP en-tête « : ". Ceci contient une chaîne encodée qui contient des détails concernant l'utilisateur/domaine.

Si vous développez la Proxy-autorisation > le NTLMSSP, vous verrez les informations décodées introduites les données NTLM. Dans le « type de message NTLM », vous noterez que c'est « NTLMSSP_NEGOTIATE ». C'est la première étape dans 3 la prise de contact de la manière NTLM.

#17 que le proxy répond avec encore 407. Des autres « proxy-authentifient » l'en-tête sont présents. Cette fois contenant une chaîne de défi NTLM. Si vous le développez plus loin, vous verrez que le type de message NTLM est « NTLMSSP_CHALLENGE ». C'est la deuxième étape

dans 3 la prise de contact de la manière NTLM.

Dans l'authentification NTLM, le contrôleur de domaine windows envoie une chaîne de défi au client. Le client applique alors un algorithme au défi NTLM factorisant dans le mot de passe d'utilisateurs dans le processus. Ceci permet au contrôleur de domaine pour vérifier que le client connaît le mot de passe correct sans envoyer jamais le mot de passe à travers la ligne. C'est beaucoup plus puis les qualifications de base sécurisées, en lesquelles le mot de passe est introduit le texte brut pour que tous les périphériques de reniflement voient.
#18 que le client envoie une finale OBTIENNENT. Notez que cet GET est sur le MÊME socket de TCP que que les NTLM négocient et le défi NTLM s'est produit sur. C'est essentiel au processus NTLM. La prise de contact entière doit se produire sur le MÊME socket de TCP, autrement l'authentification sera non valide.

Dans cette demande le client envoie le défi modifié NTLM (réponse NTLM) au proxy. C'est la dernière étape dans 3 la prise de contact de la manière NTLM.
#20 le proxy renvoie une réponse de HTTP. Ceci signifie que le proxy a reçu les qualifications et a décidé de servir le contenu.