Que deve o olhar da autenticação de NTLM como no pacote nivelar?

Índice

Introdução

Este original descreve a autenticação do gerenciador de LAN de NT (NTLM) a nível do pacote.

Que deve o olhar da autenticação de NTLM como no pacote nivelar?

Uma captura de pacote de informação para seguir este artigo pode ser transferida aqui: https://supportforums.cisco.com/sites/default/files/attachments/document/ntlm_auth.zip

IP de cliente: 10.122.142.190

IP WSA: 10.122.144.182

Número e detalhes do pacote

#4 o cliente envia um pedido GET ao proxy.

#7 o proxy envia para trás uns 407. Isto significa que o proxy não permite o tráfego devido a uma falta da autenticação apropriada. Se você olha os cabeçalhos HTTP nesta resposta, você verá “Proxy-para autenticar: NTLM”. Isto diz ao cliente que um método de autenticação aceitável é NTLM. Igualmente, se o encabeçamento “Proxy-autentica: Básico” esta presente, o proxy diz ao cliente que as credenciais básicas são aceitáveis. Se ambos os encabeçamentos estam presente (terra comum), o cliente decide que método de autenticação usará.

Uma coisa a notar é que o cabeçalho de autenticação é “Proxy-autentica: ". Isto é porque a conexão na captação usa o proxy dianteiro explícito. Se este era um desenvolvimento do proxy transparente, o código da resposta seria 401 em vez de 407 e os encabeçamentos seriam “WWW-autenticam: ” em vez de “proxy-autentique: ".

#8 o proxy FIN este soquete TCP. Isto é correto e normal.

#15 em um soquete novo TCP o cliente executa um outro pedido GET. Esta observação do tempo que o GET contém proxy-autorização do cabeçalho HTTP “: ". Isto contém uma corda codificada que contenha detalhes em relação ao usuário/domínio.

Se você expande a Proxy-autorização > o NTLMSSP, você verá a informação descodificada enviada nos dados NTLM. “No tipo de mensagem NTLM”, você observará que é

“NTLMSSP_NEGOTIATE”. Esta é a primeira etapa no aperto de mão tripartido NTLM.

#17 o proxy responde com uns outros 407. Outros “proxy-autenticam” o encabeçamento estam presente. Esta vez contém uma corda do desafio NTLM. Se você o expande mais, você verá que o tipo de mensagem NTLM é “NTLMSSP_CHALLENGE”. Este é o segundo passo no aperto de mão tripartido NTLM.

Na autenticação de NTLM, o controlador de domínio de Windows envia uma corda do desafio ao cliente. O cliente aplica então um algoritmo ao desafio NTLM que fatora na senha de usuário no processo. Isto permite que o controlador de domínio verifique que o cliente conhece a senha correta sem nunca enviar a senha através da linha. Isto é muito mais seguro do que as credenciais básicas, em que a senha é enviada no texto simples para que todos os dispositivos de farejamento considerem.

#18 o cliente envia um GET final. Note que este GET está no MESMO soquete TCP que que o NTLM negocia e o desafio NTLM ocorreu em. Isto é vital ao processo NTLM. O aperto de mão inteiro deve ocorrer no MESMO soquete TCP, se não a autenticação será inválida.

Neste pedido o cliente envia o desafio alterado NTLM (resposta NTLM) ao proxy. Esta é a etapa final no aperto de mão tripartido NTLM.

#21 o proxy envia para trás uma resposta HTTP. Isto significa que o proxy aceitou as credenciais e decidiu-o servir acima o índice.