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

Índice

Pergunta:

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

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

Número/detalhes do pacote:

#4 o cliente envia um pedido GET ao proxy

#6 o proxy envia para trás uns 407. Isto significa que o proxy não está permitindo 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” estou presente, o proxy seria dizendo ao cliente que as credenciais básicas são aceitáveis. Se ambos os encabeçamentos estam presente (terra comum), o cliente decidirá 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 está usando 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 TCP novo 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 de 3 maneiras NTLM.

#17 o proxy responde com uns outros 407. Outros “proxy-autenticam” o encabeçamento estam presente. Esta vez que contém uma corda do desafio NTLM. Se você a expande mais, você verá que o tipo de mensagem NTLM é “NTLMSSP_CHALLENGE”. Este é o segundo passo no aperto de mão de 3 maneiras NTLM.

Na autenticação de NTLM, o controlador do domínio do Windows envia uma corda do desafio ao cliente. O cliente aplica então um algoritmo ao desafio NTLM que fatora na senha de usuários 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. Esta é então umas credenciais básicas muito mais seguras, 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 de 3 maneiras NTLM.
#20 o proxy envia para trás uma resposta HTTP. Isto significa que o proxy aceitou as credenciais e decidiu-o servir acima o índice.