¿Qué debe el parecer de la autenticación NTLM en el paquete nivelar?

Contenido

Pregunta:

¿Qué debe el parecer de la autenticación NTLM en el paquete nivelar?

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

Número/detalles del paquete:

#4 el cliente envía una petición get al proxy

#6 el proxy devuelve 407. Esto significa que el proxy no está permitiendo el tráfico debido a una falta de autenticación adecuada. Si usted mira los encabezados HTTP en esta respuesta, usted verá “Proxy-para autenticar: NTLM”. Esto dice a cliente que un método de autenticación aceptable es NTLM. Asimismo, si la encabezado “Proxy-autentica: Básico” era el presente, el proxy sería diciendo al cliente que las credenciales básicas son aceptables. Si ambas encabezados están presentes (común), el cliente decidirá qué método de autenticación utilizará.

Una cosa a observar es que es el encabezado de autenticación “Proxy-autentica: ”. Esto es porque la conexión en la captura está utilizando el proxy delantero explícito. Si esto fuera un despliegue del proxy transparente, el código de la respuesta sería 401, en vez de 407, y las encabezados serían “WWW-autentican: ” en vez de “proxy-autentique: ”.

#8 el proxy FIN este socket TCP. Esto es correcto y normal.

#15 en un nuevo socket TCP el cliente realiza otra petición get. Este aviso del tiempo que el GET contiene encabezado HTTP la “proxy-autorización: ”. Esto contiene una cadena codificada que contenga los detalles con respecto el usuario/al dominio.

Si usted amplía la Proxy-autorización > NTLMSSP, usted verá la información decodificada enviada en los datos NTLM. En el “Tipo de mensaje NTLM”, usted notará que es “NTLMSSP_NEGOTIATE”. Éste es el primer paso en el apretón de manos de 3 maneras NTLM.

#17 el proxy responde con otros 407. Otros “proxy-autentican” la encabezado están presentes. Esta vez que contiene una cadena del desafío NTLM. Si usted la amplía más lejos, usted verá que el Tipo de mensaje NTLM es “NTLMSSP_CHALLENGE”. Éste es el segundo paso en el apretón de manos de 3 maneras NTLM.

En la autenticación NTLM, el regulador del Dominio de Windows envía una cadena del desafío al cliente. El cliente entonces aplica un algoritmo al desafío NTLM que descompone en factores en la contraseña de usuarios en el proceso. Esto permite que el controlador de dominio verifique que el cliente conozca la contraseña correcta sin nunca el envío de la contraseña a través de la línea. Ésta es entonces credenciales básicas mucho más seguras, en las cuales la contraseña se envía en el sólo texto para que todos los dispositivos sabueso consideren.
#18 el cliente envía un GET final. Observe que este GET está en el MISMO socket TCP que el NTLM negocia y el desafío NTLM ocurrió en. Esto es vital al proceso NTLM. El apretón de manos entero debe ocurrir en el MISMO socket TCP, si no la autenticación será inválida.

En esta petición el cliente envía el desafío modificado NTLM (respuesta NTLM) al proxy. Éste es el último paso en el apretón de manos de 3 maneras NTLM.
#20 el proxy devuelve un HTTP de respuesta. Esto significa que el proxy validó las credenciales y ha decidido a servir para arriba el contenido.