패킷 수준에서 NTLM 인증은 어떤 형태로 나타납니까?

TAC **문서 ID: 117931**

기고자: Josh Wolfer 및 Jeff Richmond, Cisco TAC 엔지니어 2014년

7월 14일

목차

질문:

패킷 수준에서 NTLM 인증은 어떤 형태로 나타납니까?

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

패킷 번호/세부 사항:

#4 클라이언트에서 GET 요청을 프록시로 보냅니다.

#6 프록시에서 407을 다시 보냅니다. 이는 적절한 인증이 이루어지지 않아 프록시에서 해당 트래픽을 허용하지 않음을 의미합니다. 이 응답의 HTTP 헤더를 보면 "Proxy−authenticate: NTLM"이라고 표시되어 있습니다. 이는 허용되는 인증 방법이 NTLM이라는 사실을 클라이언트에 알려주는 것입니다. 이와 마찬가지로, 헤더가 "Proxy−authenticate: Basic"인 경우 프록시에서는 기본 자격 증명이 허용된다는 사실을 클라이언트에 전달합니다. 두 가지 헤더가 모두 존재할 경우(이런 경우가 많음), 클라이언트에서는 어떤 인증 방법을 사용할지 결정합니다.

인증 헤더는 "Proxy−authenticate:"로 시작한다는 점을 기억해두십시오. 이는 캡처 중인 연결에서 명시적 전달 프록시를 사용하고 있기 때문입니다. 투명 프록시 배포의 경우 응답 코드는 407이 아닌 401이며, 헤더는 "proxy−authenticate:"가 아닌 "www−authenticate:"입니다.

#8 프록시에서 이 TCP 소켓을 FIN합니다. 이는 올바르며 정상적인 상태입니다.

#15 새로운 TCP 소켓에서 클라이언트가 다른 GET 요청을 수행합니다. 이 경우 GET에는 HTTP 헤더 "proxy−authorization:"이 포함됩니다. 여기에는 사용자/도메인과 관련된 세부 정보가 담긴 인코딩된 문자열이 포함됩니다.

Proxy−authorization(프록시−인증) > NTLMSSP로 확장할 경우 NTLM 데이터로 전송된 디코딩된 정보가 표시됩니다. "NTLM Message Type"(NTLM 메시지 유형)을 보면 "NTLMSSP_NEGOTIATE"로 되어 있습니다. 이는 3방향 NTLM 핸드셰이크의 첫 번째 단계입니다.

#17 프록시에서 또 다른 407에 응답합니다. 또 다른 "proxy−authenticate" 헤더가 존재합니다. 이번에는

NTLM 챌린지 문자열이 포함됩니다. 더 확장할 경우 NTLM 메시지 유형이 "NTLMSSP_CHALLENGE"로 표시됩니다. 이는 3방향 NTLM 핸드셰이크의 두 번째 단계입니다.

NTLM 인증에서 Windows 도메인 컨트롤러는 챌린지 문자열을 클라이언트에 전송합니다.

클라이언트에서는 사용자 비밀번호가 처리되는 과정에서 NTLM 챌린지 인수 분해에 알고리즘을 적용합니다. 이렇게 하면 도메인 컨트롤러에서는 라인 전체에 비밀번호를 보내지 않고도 클라이언트에서 정확한 비밀번호를 알고 있는지를 확인할 수 있습니다. 이 방법은 비밀번호가 일반 텍스트로 전송되어 모든 도청 장치에 표시될 수 있는 기본 자격 증명보다 훨씬 안전합니다.
#18 클라이언트에서 마지막 GET 요청을 보냅니다. 이 GET 요청은 NTLM 협상 및 NTLM 챌린지가 발생한 것과 동일한 TCP 소켓에서 발생합니다. 이는 NTLM 프로세스에서 매우 중요합니다. 전체 핸드셰이크는 동일한 TCP 소켓에서 발생해야 하며, 그렇지 않을 경우 인증이 무효화됩니다.

이 요청에서 클라이언트는 수정된 NTLM 챌린지(NTLM 응답)를 프록시에 전송합니다. 이는 3방향 NTLM 핸드셰이크의 마지막 단계입니다.
#20 프록시에서 HTTP 응답을 다시 보냅니다. 이는 프록시에서 자격 증명을 수락했으며 콘텐츠를 지원하도록 결정했음을 의미합니다.

업데이트 날짜: 2014년 7월 14일 문서 ID: 117931
