패킷 수준에서 NTLM 인증은 어떻게 표시되어야 합니까?

목차

소개

이 문서에서는 패킷 수준에서 NTLM(NT LAN Manager) 인증에 대해 설명합니다.

패킷 수준에서 NTLM 인증은 어떻게 표시되어야 합니까?

이 문서를 팔로우할 패킷 캡처는 여기에서 다운로드할 수 있습니다.
https://supportforums.cisco.com/sites/default/files/attachments/document/ntlm_auth.zip

클라이언트 IP:10.122.142.190

WSA IP:10.122.144.182

패킷 번호 및 세부 정보

#4 클라이언트가 프록시에 GET 요청을 보냅니다.

#7 프록시가 407을 다시 보냅니다. 즉, 적절한 인증이 없어 프록시가 트래픽을 허용하지 않습니다.이 응답에서 HTTP 헤더를 보면 "Proxy-authenticate:NTLM". 이는 허용 가능한 인증 방법이 NTLM임을 클라이언트에 알립니다.마찬가지로 헤더 "Proxy-authenticate:Basic(기본)"이 있으며, 프록시는 기본 자격 증명이 허용됨을 클라이언트에 알립니다.두 헤더가 모두 있는 경우(공통) 클라이언트는 어떤 인증 방법을 사용할지 결정합니다.

한 가지 주목할 점은 인증 헤더가 "Proxy-authenticate:"라는 것입니다. 캡처의 연결에서 명시적 전달 프록시를 사용하기 때문입니다.투명 프록시 구축인 경우 응답 코드는 407 대신 401이고 헤더는 "proxy-authenticate:" 대신 "www-authenticate:"가 됩니다.

#8 이 TCP 소켓의 프록시 FIN입니다.이것은 정확하고 정상이다.

#15 클라이언트가 새 TCP 소켓에서 다른 GET 요청을 수행합니다.GET에 HTTP 헤더 "proxy-authorization:"이 포함되어 있습니다. 사용자/도메인에 대한 세부 정보를 포함하는 인코딩된 문자열을 포함합니다.

Proxy-authorization > NTLMSSP를 확장하면 NTLM 데이터에서 디코딩된 정보가 표시됩니다."NTLM Message Type(NTLM 메시지 유형)"에서 "NTLMSSP_NEGOTIATE"입니다. 이는 3방향 NTLM 핸드셰이크의 첫 번째 단계입니다.

#17 프록시가 다른 407에 응답합니다. 다른 "proxy-authenticate" 헤더가 있습니다.이번에는 NTLM

챌린지 문자열을 포함합니다.더 확장하면 NTLM 메시지 유형이 "NTLMSSP_CHALLENGE"인 것을 볼 수 있습니다. 3방향 NTLM 핸드셰이크의 두 번째 단계입니다.

NTLM 인증에서 Windows 도메인 컨트롤러는 클라이언트에 챌린지 문자열을 전송합니다.그런 다음 클라이언트는 NTLM 챌린지에 알고리즘을 적용합니다. 이 문제는 프로세스 중 사용자의 비밀번호를 좌우합니다.이렇게 하면 도메인 컨트롤러가 회선을 통해 비밀번호를 전송하지 않고 클라이언트가 올바른 비밀번호를 알고 있는지 확인할 수 있습니다.이는 모든 스니핑 디바이스가 볼 수 있도록 비밀번호가 일반 텍스트로 전송되는 기본 자격 증명보다 훨씬 안전합니다.

#18 클라이언트가 최종 GET을 전송합니다.이 GET은 NTLM Negotiate 및 NTLM Challenge(NTLM 협상 및 NTLM 챌린지)가 발생한 것과 동일한 TCP 소켓에 있습니다.이는 NTLM 프로세스에 매우 중요합니다.전체 핸드셰이크가 동일한 TCP 소켓에서 발생해야 합니다. 그렇지 않으면 인증이 유효하지 않습니다.

이 요청에서 클라이언트는 수정된 NTLM Challenge(NTLM Response)를 프록시에 전송합니다.3방향 NTLM 핸드셰이크의 마지막 단계입니다.

#21 프록시가 HTTP 응답을 다시 전송합니다.이는 프록시가 자격 증명을 수락하고 콘텐츠를 서비스하기로 결정했음을 의미합니다.