什么是NTLM验证

NTLM验证是在Windows NT时代引入的验证方式，目前已逐步被Kerberos取代。但是为了应用程序的兼容性，目前所有操作系统都提供NTLM支持。

NTLM验证流程

1. 客户端提供明文用户名给目标服务器
2. 目标服务器产生16 byte的随机码返回给客户端，称为challenge
3. 客户端采用自己密码生成的密钥加密该challenge并返回给服务器，称为response
4. 服务器发送如下内容给域控：

* 用户名
* Challenge
* Response

1. 域控采用用户名查找数据库并获得密码，并用该密钥加密challenge
2. 域控比较加密后的challenge和服务器发送的response，如果一致，则验证通过

需要注意的是，验证信息是由服务器（而不是客户端）发送给域控，这是与Kerberos最大的区别。

NTLM验证排错

1. Netlogon debug日志

nltest /dbflag:0x2080ffff

C:\windows\debug\netlogon.log and netlogon.bak

1. 网络抓包