Disabling NTLM Authentication in Windows Domain

In this article, we will explore the topic of disabling NTLM authentication in a Windows domain environment. NTLM (NT LAN Manager) authentication is an outdated authentication protocol that has security vulnerabilities. Disabling NTLM authentication is important for improving the security posture of a Windows domain and ensuring that only more secure authentication protocols, such as Kerberos, are used.

NTLM authentication is commonly used in Windows environments for authenticating users and granting access to resources. However, it has several weaknesses, including the storage of passwords in a less secure format and susceptibility to various attacks, such as pass-the-hash and pass-the-ticket attacks.

To disable NTLM authentication in a Windows domain, follow these steps:

1. Open the Group Policy Management Console on a domain controller.
2. Create a new Group Policy Object (GPO) or edit an existing one.
3. Navigate to Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Security Options.
4. Locate the "Network security: Restrict NTLM: Incoming NTLM traffic" policy and set it to "Deny All".
5. Locate the "Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers" policy and set it to "Deny All".
6. Apply the GPO to the desired Organizational Units (OUs) or to the entire domain.

By applying these policies, NTLM authentication will be disabled, and only more secure authentication protocols, such as Kerberos, will be allowed. It is important to note that before disabling NTLM authentication, you should ensure that all applications and services in your environment are compatible with Kerberos authentication or any alternative authentication mechanism you plan to use.

Example:

To disable NTLM authentication using PowerShell, you can use the following command:

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0"
 -Name "RestrictSendingNTLMTraffic" -Value 2
```

This command modifies the registry value to restrict the sending of NTLM traffic.