Restrict NTLM Incoming traffic

August 3, 2021

NTLM is Microsoft's old mythological authentication protocol. Although new and better authentication protocol has already been developed, NTLM is still very much in use. Even the most recent Windows versions support NTLM and even Active Directory is required for default NTLM implementation. NTLM protocol has proven to have many flaws that result in potential vulnerabilities. Our main conclusion from this situation is that the best way to protect your organization from NTLM vulnerabilities is in fact, not to use it!

Policy Description:

Although disabling NTLM in every machine in the network may be the ideal solution, it is almost always impossible. One caution measure that can be taken is restricting NTLM incoming traffic, which is a fundamental step in a hardening project. This policy will allow you to deny or allow incoming NTLM traffic.

Hardening can be a painful procedure when done in complex environments. If you are reading this article, you probably know it. Endless hours and resources are invested in this task. However, despite the efforts, hardening often causes downtime. In fact, over 60% of IT professionals report they've experienced downtime while trying to harden their infrastructure*.

After years of hardening using the traditional manual tools, we concluded that using hardening automation tools is essential for achieving a successful hardening project and a good compliance posture. Learn more about server hardening automation.

This post aims to provide basic information and configuration recommendations for setting NTLM incoming traffic rules. After deciding your policy, make sure to test it before enforcing it, to make sure it will not cause damage.

Potential vulnerability - PetitPotam:

PetitPotam is a vulnerability that uses NTLM's remote authentication protocol- EFSRPC. This vulnerability eventually allows attackers to perform an NTLM relay attack and completely take over a Windows domain.

An attacker requests to connect with a Domain Controller via the EFSPRC and forces it to use NTLM (instead of Kerberos or more secure authentication mechanisms). Once the authentication is done using NTLM, the attacker performs a classic NTLM relay to grab the hashed password.

The attack usually targets IIS servers installed on the Domain Controller and is used for certificate service web enrollment. Once the attacker has domain credentials, he breaches the web enrollment, gets the certificate, and gains control over the domain.

Restricting NTLM incoming traffic is a good option when you want to protect yourself from PetitPotam, but can’t disable NTLM in the entire network.

PetitPotam Vulnerability Severity:

Critical.

Default Value:

Not Defined.

CalCom Recommended Value:

Deny all accounts.

The Potential Impact of Changing restricting NTLM incoming traffic:

Policy set to “Allow all” or do not configured: the server will allow all NTLM authentication requests.

Policy set to “Deny all domain accounts”: the server will deny NTLM authentication requests for domain logon and display an NTLM blocked error, but allow local account logon.

Policy set to “Deny all accounts”: the server will deny NTLM authentication requests from incoming traffic and display an NTLM blocked error.

This setting allows you to control where NTLM is being used and to enable it only if required. Before changing this setting, you need to either manually map NTLM and perform an impact analysis, or use a hardening automation tool to save time and resources.

HOW TO CONFIGURE:

Policy path:

Computer Configuration\Windows Settings\Local Policies\Security Options

Registry settings:

MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\RestrictReceivingNTLMTraffic