How to Disable Null Sessions in Windows (and Why You Should)

How to Disable Windows Null Sessions

In a Windows environment, null sessions can allow users to have anonymous access to hidden administrative shares on a system. Once connected to the shares through a null session, attackers can potentially enumerate information about your system and environment, such as users and groups, operating systems, password policies, privileges, etc. With this information, an attacker can learn about any potential vulnerabilities or ways to best attack your systems. Disabling null sessions is a key way to help you strengthen your organization's security and reduce your attack surface.

Edit GPO- Go to Computer configuration\Policies\Windows settings\Security Settings\Local Policies\SecurityOptions

Enable:

- Network access: Restrict Anonymous access to Named Pipes and Shares
- Network access: Do not allow anonymous enumeration of SAM accounts
- Network access: Do not allow anonymous enumeration of SAM accounts and shares
- Network access: Shares that can be accessed anonymously

Disable:

- Network access: Let Everyone permissions apply to anonymous users
- Network access: Allow anonymous SID/Name translation
- Restrict Null Sessions in the Registry

If you open regedit and browse to:

- HKLM\System\CurrentControlSet\Control\Lsa\RestrictAnonymous
  1 - Null sessions can not be used to enumerate shares
- HKLM\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM
  1 - Default setting. Null sessions can not enumerate user names
- HKLM\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous
  0 - Default setting. Null sessions have no special rights

Figure 1: Modifying the RestrictAnonymous key in the registry

Disable smbv1 via PowerShell

There are a wide variety of exploits for smbv1. Follow recommended settings and steps via the Microsoft Support article for your Operating System. Sources:

- How to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows
- Disable null sessions on domain controllers and member servers

Protect Your Windows Environment

Blumira makes security easy and effective for SMBs and mid-market companies, helping them detect and respond to cybersecurity threats faster to stop breaches and ransomware. Blumira's all-in-one SIEM platform combines logging with automated detection and response for better security outcomes and consolidated security spend. Get your trial account with Blumira and secure your Microsoft 365 environment in minutes. No credit card required.

Additional Security Resources

View All Posts
Read More
Read More
Read More