REPORT
System Hardening via Local GPO: Restricting Anonymous Connections

v1.0.0

Author:

Eldon Gabriel

September 30, 2025

TABLE OF CONTENTS

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.0.0	09/30/2025	Eldon G.	Initial draft.

I. INTRODUCTION AND PROJECT SCOPE

1.1 Project Description

This project was performed on a Windows 10 computer using the Local Group Policy (`gpedit.msc`). The aim is to stop unknown users from accessing system details without permission.

Disclaimer: This report documents my personal work completing an MCSI lab exercise. It reflects my understanding and configuration of Windows 10 Local Group Policy settings for operating system patching in a controlled, offline environment. No MCSI instructional videos, lab guides, or proprietary materials have been posted, shared, or distributed. The content has been written independently to demonstrate my skills while remaining fully compliant with MCSI's academic pledge and policies.

1.2 Security Goals

The goal is to make the system safer by stopping features that allow unknown users to use system resources without logging in.

1.3 Objectives

1. Disable anonymous SID/Name translation.
2. Block enumeration of SAM accounts and shares.
3. Restrict anonymous access to named pipes and shared resources.
4. Deny network access to local accounts.
5. Enforce secure client/server authentication.

1.4 Portfolio Value

This work shows skill in making Windows more secure, managing the Group Policy, and protecting systems from being spied on.

II. THREAT BACKGROUND AND RATIONALE

2.1 Threat of Anonymous Connections (Null Sessions)

A null session is a legacy feature that allows remote connections without credentials. Attackers exploit null sessions to enumerate system information without any authentication.

2.2. Adversary Reconnaissance (the "Why")

Through anonymous connections, attackers can:

- Enumerate the users and groups.
- Translate SIDs into usernames.
- Shared resources and named pipes were discovered.
- Gather OS and policy information on targeted attacks.

2.3. Control Mechanism

Disabling anonymous access via the Local Group Policy enhances security. This aligns with the CIS Benchmarks and Microsoft standards.

III. GPO IMPLEMENTATION

3.1. Implementation Environment

Operating System: Windows 10

Tool: Local Group Policy Editor (gpedit.msc)

3.2. Configuration Matrix: Anonymous Access Restrictions

Policy: Network access: Allow anonymous SID/Name translation

Path: Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options

Configured State: Disabled

Policy: Network access: Do not allow anonymous enumeration of SAM accounts

Path: Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options

Configured State: Enabled

Policy: Network access: Do not allow anonymous enumeration of SAM accounts and shares

Path: Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options

Configured State: Enabled

Policy: Network access: Let Everyone permissions apply to anonymous users

Path: Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options

Configured State: Disabled

Policy: Network access: Restrict anonymous access to Named Pipes and Shares

Path: Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options

Configured State: Enabled

Policy: Network security: Allow Local System to use computer identity for NTLM

Path: Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options

Configured State: Enabled

Policy: Network security: Allow LocalSystem NULL session fallback

Path: Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options

Configured State: Disabled

3.3. Configuration Matrix: Client/Server Behavior Controls

Policy: Enable insecure guest logons

Path: Computer Configuration → Administrative Templates → Network → Lanman Workstation

Configured State: Disabled

3.4. Configuration Matrix: User Rights Denial

Policy: Deny access to this computer from the network

Path: Computer Configuration → Windows Settings → Security Settings → Local Policies → User Rights Assignment

Principal Added: NT AUTHORITY\Local Account

IV. TECHNICAL VERIFICATION

4.1. Policy Application

The `gpupdate/force` command was executed to apply the changes immediately.

4.2. Verification Method

Registry queries and the Local Security Policy snap-in were used to confirm hardened states.

4.3. Demonstration of Hardening

To confirm that the null session restrictions were active, I queried the registry directly.

```cmd
reg query HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameter
RestrictNullSessAccess
```

Result:

```cmd
RestrictNullSessAccess REG_DWORD 0x1
```

The `0×1` value confirms that **restricting anonymous access to Named Pipes and Shares** is successfully enforced. An anonymous attempt to list items from another computer was stopped, showing that null sessions were no longer allowed.

4.4. Conclusion of Verification

Anonymous connections were successfully disabled in this study. The workstation now operates with hardened security baselines that prevent unauthenticated reconnaissance.

V. CONCLUSION

5.2 Key Takeaways

All necessary Local Group Policy settings were set up. This prevented the system details from being listed anonymously.

Learning Outcomes

- Direct link between Group Policy settings and underlying registry configuration.

- Understanding how system baselines mitigate adversary reconnaissance techniques.

5.2 Security Implications and Recommendations

- Monitor system security logs for failed anonymous logon attempts.
- Hardening is strengthened by adding identity rules, limiting NT LAN Manager (NTLM), and using Kerberos authentication.
- Replicate the configuration across enterprise systems using domain-level GPOs.
