SOP
Restricting Anonymous Connections & Reconnaissance Hardening

v1.0.0

Author:
Eldon Gabriel

March 21, 2025

Table of Contents

Disclaimer: This report documents my personal work completing an MCSI lab exercise. It reflects the author’s 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

Revision History

Version	Date	Author	Description of Changes
1.0.0	09/30/2025	Eldon G.	Initial draft.
1.0.1	03/21/26	Eldon G.	Aligned reconnaissance mitigation with NIST 800-53 (AC-14) and MITRE ATT&CK (T1087); established a hardened baseline against null sessions; verified via registry-level auditing and enumeration testing.

Executive Summary

Project Overview

Restricting Anonymous Connections & Reconnaissance Hardening

This project focused on securing a Windows system by blocking anonymous access (null sessions). The goal was to prevent unauthenticated users from viewing system details, such as user accounts, shared folders, and network resources.

Project Objective

The main goal is to reduce the risk of attackers gathering information during the early stages of an attack. By disabling anonymous access to system data, the system no longer reveals useful details that can help an attacker plan the next steps.

This helps prevent:

- User account discovery
- Network share enumeration
- Exposure of system configuration data

Technical Implementation

The system was secured using the following controls:

- **Null Session Restriction:** Blocked anonymous users from listing accounts and shared resources
- **Registry Hardening:** Restricted access to registry paths that could expose system data
- **Policy Enforcement:** Enabled settings like RestrictAnonymous and NoEnumeration to deny all unauthenticated requests
- **Framework Alignment:** Mapped controls to NIST 800-53 (AC-14) and MITRE ATT&CK (Account Discovery)

Validation and Testing

To confirm that the system was secure, the following tests were performed:

- **Enumeration Testing:** Attempted to list users and shares without authentication and confirmed access was denied
- **Registry Verification:** Checked registry settings to ensure policies were correctly applied
- **Policy Persistence:** Used `gpupdate /force` to confirm settings remained active after refresh

1.0 Introduction and Project Scope

1.1 Project Description

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

1.2 Security Goals

The goal is to enhance system safety by preventing unknown users from accessing 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. Ensure secure client/server authentication.

1.4 Portfolio Value

This work demonstrates skills in enhancing Windows security, managing Group policies, and protecting systems from being spied on.

2.0 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

- Count the number of users and groups.
- Translate SIDs to usernames.
- Shared resources and named pipes have been discovered.
- Collect 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.

3.0 GPO Implementation

3.1. Implementation Environment

The configuration was performed on a Windows 10 workstation using a **Local Group Policy Editor** (`gpedit.msc`).

3.2. Configuration Summary

Anonymous Access Restrictions

A series of security policies were applied to remove the ability of unauthenticated users to perform reconnaissance against the system. These controls focused on:

1. **Disabling translation and enumeration features** that allow the discovery of local accounts, groups, and system identifiers.

2. **Restricting insecure network behaviors**, including legacy fallback mechanisms and permissive access models

3. **Implement access denial rules** for non-privileged accounts to prevent local accounts from being abused for remote sessions.

3.3. Policy Grouping

In total, **11 policies** were set across the **Security Options**, **Administrative Templates**, and **User Rights Assignment** categories. Collectively, these policies blocked anonymous SID/name translation, prevented the enumeration of SAM accounts and shares, restricted insecure NTLM usage, and denied unauthorized accounts from remotely connecting.

This layered approach eliminates the primary pathways for null session exploitation without impacting normal authenticated system use.

4.0 Technical Verification and Proof of Work

4.1. Policy Application

After configuration, the settings were enforced immediately using the `gpupdate /force` command to ensure that all changes were active.

4.2. Verification Method

Validation was performed using a combination of methods.

- **Registry queries** to confirm that the underlying system values had been updated to match the intended security posture.
- **Enumeration attempts** (e.g., user-and-share listing tests) were conducted to prove that anonymous connections no longer produce results.

4.3. Demonstration of Hardening

Before configuration, anonymous sessions could return accounts or share data; these queries are now blocked, demonstrating that the system successfully enforces the new restrictions. Registry checks confirmed that the relevant keys reflected the hardened state.

4.4. Conclusion of Verification

The verification process confirmed that the workstation was operating under a **hardened baseline**, resisting reconnaissance through unauthorized anonymous connections.

5.0 Conclusion

5.1 Key Takeaways

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

Learning Outcomes

- Direct link between Group Policy settings and the underlying registry configuration.
- Understanding how system baselines mitigate adversary reconnaissance techniques

5.2 Security Implications and Recommendations

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