



REPORT

SMB Hardening for

Credential Theft

Protection

v1.0.0

Author:

Eldon Gabriel

October 13, 2025



TABLE OF CONTENTS


REVISION HISTORY.....	2
1.0 EXECUTIVE SUMMARY.....	3
1.1 Objective.....	3
1.2 Action Taken.....	3
1.3 Result.....	3
2.0 BACKGROUND AND RISK ANALYSIS.....	4
2.1 Threat.....	4
2.2 Vulnerability.....	4
2.3 Security Principle.....	4
3.0 IMPLEMENTATION AND CONFIGURATION.....	5
3.1 Tooling Used.....	5
3.2 Configuration Steps (Policy Settings).....	5
3.3 Registry Modification (Disable SMBv1).....	5
4.0 TECHNICAL RATIONALE AND IMPACT.....	6
4.1 SMB Signing.....	6
4.2 Idle Session Timeout.....	6
4.3 Mitigation of SMBv1.....	6
5.0 CONCLUSION.....	7
2.1 Key Takeaways.....	7
2.2 Security Implications and Recommendations.....	7

Disclaimer: This report documents my personal work completing an MCSI lab exercise. It reflects my independent understanding and configuration of Windows 10 Local Group Policy settings in a controlled environment. No MCSI video content, lab materials, or proprietary instructions have been shared or distributed. All information presented follows MCSI's disclosure and academic integrity policies.



Cybersecurity Professional | IT Security Consultant

REVISION HISTORY

Version	Date	 Author	Description of Changes
v1.0.0	10/13/2025	Eldon G.	Initial draft.





1.0 EXECUTIVE SUMMARY

1.1 Objective

This exercise aimed to protect a Windows Virtual Machine (VM) from attempts to steal login credentials and take over sessions using the Server Message Block (SMB) protocol.

1.2 Action Taken

A Local Group Policy Object (LGPO) was deployed to enforce SMB signing for both client and server communication. Additionally, SMBv1 was disabled in the Windows Registry to remove legacy protocol vulnerabilities.

1.3 Result

The system now requires a digital signature for all SMB traffic. It blocks any exchange of passwords that are not encrypted and automatically ends inactive sessions. This stops major ways of stealing credentials and taking over SMB sessions. This setup reduces the chance of someone taking over a session or stealing login details through methods such as relay attacks and packet interception.



2.0 BACKGROUND AND RISK ANALYSIS

2.1 Threat

Individuals who can view network traffic may misuse unsecured SMB sessions. They can use tools such as **Responder** or **SMB Relay** to capture login details and pretend to be real users. These attacks catch or change SMB packets to obtain password hashes or act like real users.

2.2 Vulnerability

Unsecured SMB traffic may allow clear-text password exchanges or unsigned sessions. Without integrity checks, attackers can inject or replay packets to obtain unauthorized access. Older SMB versions, especially SMBv1, are also known to contain critical flaws that are exploited in attacks such as *WannaCry* and *EternalBlue*.

2.3 Security Principle

This exercise uses the concepts of **Defense in Depth**, **Least Functionality**, and **Cryptographic Integrity Enforcement**. By signing SMB traffic and turning off old protocols, communication is made more secure, and devices are better protected.



3.0 IMPLEMENTATION AND CONFIGURATION

3.1 Tooling Used

- Local Group Policy Editor (`gpedit.msc`)
- Registry Editor (`regedit`)
- Command Prompt (`gpupdate /force`)

3.2 Configuration Steps (Policy Settings)

Client Policies

- *Microsoft network client: Digitally sign communications (always)* → **Enabled**
- *Microsoft network client: Digitally sign communications (if server agrees)* → **Enabled**
- *Microsoft network client: Send unencrypted password to third-party SMB servers* → **Disabled**

Server Policies

- *Microsoft network server: Amount of idle time required before suspending session* → **15 minutes**
- *Microsoft network server: Digitally sign communications (always)* → **Enabled**
- *Microsoft network server: Digitally sign communications (if client agrees)* → **Enabled**

3.3 Registry Modification (Disable SMBv1)

- **Path:**
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters`
- **Value Name:** `SMB1`
- **Type:** `DWORD` (32-bit)
- **Data:** `0` This registry key disables the SMBv1 functionality on the system.



4.0 TECHNICAL RATIONALE AND IMPACT

4.1 SMB Signing

SMB signing adds a secure signature to every data packet. This ensures the data's safety and confirms the identities of both the client and server. This prevents tampering, replay, and impersonation attempts during SMB communications. It directly prevents session hijacking, replay attacks, man-in-the-middle attacks, and credential theft.

4.2 Idle Session Timeout

By setting a 15-minute idle timeout, unused SMB sessions are automatically suspended. This reduces the chance of attackers using inactive but logged-in sessions to gain access.

4.3 Mitigation of SMBv1

Turning off SMBv1 removes old security risks and follows the Least Functionality rule by eliminating outdated code that hackers can use. This follows the **Least Functionality** principle by removing unnecessary and insecure components.



5.0 CONCLUSION

The goal of securing SMB communications on a standalone Windows computer was achieved. All group policies and registry settings were successfully applied. This includes enforcing SMB signing, blocking unencrypted passwords, and turning off SMBv1. These steps match modern Windows security standards and help prevent common methods of stealing credentials and hijacking sessions.

5.1 Key Takeaways

- SMB signing ensures that the data is correct and secure. This allows only trusted devices to connect properly.
- Turning off SMBv1 helps eliminate old and unsafe parts of the system.
- Setting time limits for idle sessions reduces the risk of someone taking over a session and moving through the system.
- Using the Local Group Policy shows basic skills for making computers more secure. These skills are useful in both large companies and small laboratories.

5.2 Security Implications and Recommendations

- **Maintain Protocol Hygiene:** Regularly check and turn off outdated network services, such as SMBv1, Telnet, or old RPC methods.
 - **Apply Centralized Policy Management:** In business settings, use Active Directory Group Policy Objects (GPOs) to apply security rules across the network.
 - **Audit SMB Connections:** Check the event logs for any unsigned or failed SMB logins using Event Viewer → Security Logs. This can help identify possible downgrades or relay attempts.
 - **Continuous Review:** Check security settings after major Windows updates or changes to ensure they still work and follow the rules.
-