REPORT
SMB Protocol: Function and Security Risks

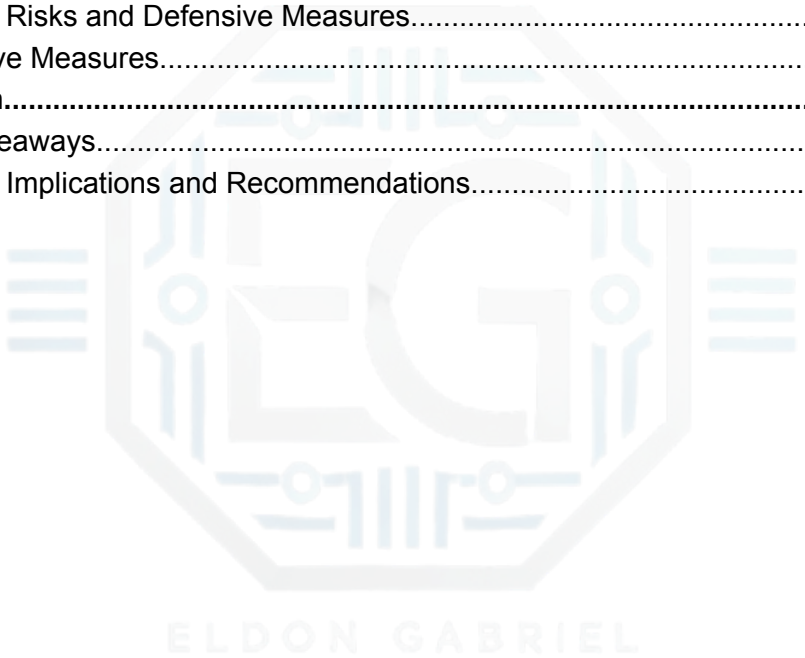
v1.1.0

Author:
Eldon Gabriel

March 29, 2025

Security Systems Specialist

Table of Contents



Disclaimer: This guide documents the authors' independent research and technical understanding of the SMB protocol and its security implications. The content is based on publicly available documentation and standard industry security practices. It does not contain proprietary MCSI lab instructions, video content, or the provided solutions. All work presented herein complies with the MCSI disclosure requirements and academic integrity policies.

Revision History

Version	Date	Author	Description of Changes
1.0.0	08/24/2025	Eldon G.	Initial draft.
1.1.0	03/29/2025	Eldon G.	Updated formatting and expanded Section 4.2 with technical guidance on SMB Signing, Encryption, and Perimeter Hardening (Port 445).

ELDON GABRIEL

0.0 Executive Summary

This report reviews the SMB protocol, which allows computers to connect over a network and share files, printers, and other resources. SMB is commonly used in organizations to help employees work together and manage tasks more efficiently. The report outlines how SMB works, its different versions, and common uses in Windows networks, including Active Directory and centralized access management.

It also highlights security risks, particularly with SMBv1, which is outdated and vulnerable to attacks, such as EternalBlue and WannaCry. The report recommends disabling SMBv1, keeping systems up to date, limiting exposure to public networks, applying firewalls, and using network segmentation. When combined with regular audits and staff training, these measures create a strong, multi-layered defense against SMB-related threats.

ELDON GABRIEL

1.0 Server Message Block (SMB) Protocol

1.1 Project Overview

Server Message Block (SMB) is a protocol that enables computers on a network to share files, printers, and other resources with one another. It allows employees in a business to work together more easily by providing quick access to shared resources. SMB is used in many organizations because it simplifies communication and file management across multiple systems.

However, SMBs also have security risks. Its wide use and complex features make it a target for cyber attackers. Past vulnerabilities in SMB have caused major security incidents, such as the WannaCry ransomware attack. Businesses must balance SMB's convenience with strong security practices. Regular updates, correct configuration, and network separation are important to reduce risks while using SMB effectively.

ELDON GABRIEL

2.0 How SMB Works

2.1 Protocol Operation

SMB works on a client-server model. The client computer requests access to files, printers, or other resources, and the server computer responds with the requested data or services. This setup allows multiple users to access shared resources on the network efficiently.

2.2 Protocol Versions

SMB has gone through several versions, each adding better performance, security, and features.

- **SMB 1.0:** The first version is outdated and insecure.
- **SMB 2.0**: Offers faster performance and reduces network traffic.
- **SMB 3.0**: Adds encryption, multichannel connections for faster data transfer, and better protection against attacks, such as man-in-the-middle attacks.

Using older versions, such as **SMB 1.0,** is not recommended because they can make networks unsafe. SMB usually communicates through **TCP ports 139 and 445**. Port 139 works with NetBIOS over TCP/IP, whereas port 445 allows computers to communicate directly without using NetBIOS. The client connects to the server on these ports and sends requests, which the server responds to for file or printer access.

3.0 Use Cases and Security Risks

3.1 Common Uses In The Real World

In Windows networks, SMB is used for file and printer sharing. It allows employees to access files across multiple computers. Windows domains use centralized authentication, which allows administrators to manage who can access different resources based on user permissions. Sharing files and printers improves collaboration in offices. Employees can work on projects together, share documents, and use shared printers without requiring extra setups.

Active Directory makes this process even better by organizing users, computers, and resources in a structured manner. It provides administrators with detailed control over access, simplifies user management, and provides a single login for all services. SMB is essential for organizations looking to improve workflows and productivity.

3.2 Security Risks and Defensive Measures

Exploits, such as EternalBlue and the WannaCry ransomware, demonstrate the dangers of vulnerable SMB systems. EternalBlue targeted a flaw in SMBv1, allowing attackers to run code on other computers. WannaCry used EternalBlue to spread across networks, encrypt files, and demand ransoms.

Owing to these risks, SMBv1 has been deprecated. SMBv1 does not have modern security features and is vulnerable to attacks. Microsoft advises using SMBv2 or SMBv3 instead. To reduce these risks, organizations should:

- ➢ Keep the systems updated with security patches.
- ➢ Limit SMB exposure, especially to the Internet.
- ➢ Disable unneeded SMB services.
- ➢ Apply firewalls to control SMB traffic in trusted networks.

3.3 Defensive Measures

Disabling SMBv1 is critical. This outdated version is easy for attackers to exploit. Organizations should verify that all systems work with SMBv2 or SMBv3 before disabling SMBv1. Blocking SMB from public networks, using firewalls, and segmenting networks also improve security. Firewalls filter and monitor SMB traffic, whereas segmentation isolates sensitive systems to prevent malware from spreading. These steps together create strong, multi-layered protection.

4.0 Conclusion

4.1 Key Takeaways

Disabling SMBv1 is essential for modern network security. SMBv1 is outdated and lacks encryption, making it risky. Organizations should verify that all devices support SMBv2 or SMBv3 before disabling SMBv1.

Blocking SMB from public networks prevents attackers from accessing the network. Firewalls and network segmentation provide additional protection by controlling traffic and isolating critical systems.

Regular security audits and employee training also help. Staff should understand SMB risks and follow safe file-sharing practices. Implementing these measures together creates a strong defense, reduces risks, and helps organizations stay secure against evolving cyber threats.

4.2 Security Implications and Recommendations

The main risk with the SMB protocol comes from using older versions, especially SMBv1, and from not encrypting data in transit in versions prior to 3.0.

These weaknesses make it easier for attackers to

- Steal login credentials
- Intercept and alter network traffic (Man-in-the-Middle attacks)
- Spread ransomware quickly across the network (like EternalBlue)

Technical Recommendations

- **Remove Old Protocols:** Check your systems for SMBv1 and disable it using Group Policy (GPO). This removes the major attack path used by the worms.
- **Use SMB Encryption:** Require SMB 3.0 or higher with encryption enabled. This protects the sensitive data while moving across the network.
- **Block External Access:** Ensure that TCP port 445 is blocked by the firewall. This prevents attackers from reaching SMB services from outside the network.
- **Enable SMB Signing:** Turn on SMB signing to confirm that the data has not changed during transmission and to reduce the risk of NTLM relay attacks.

- **Segment Network:** Place file servers and admin shares in separate VLANs. Allow only trusted systems to access them.

ELDON GABRIEL