CIS Center for Internet Security®

CIS Controls

Exploited Protocols:
Server Message Block (SMB)

Acknowledgments

The Center for Internet Security® (CIS®) would like to thank the many security experts who volunteer their time and talent to support the CIS Critical Security Controls® (CIS Controls®) and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

Editor
Valecia Stocchetti, CIS

CIS Contributors
Ginger E. Anderson
Jennifer Jarose
Phyllis Lee
Robin Regnier
Phil White
Thomas Sager

The Center for Internet Security, Inc. (CIS) is a 501(c)(3) nonprofit organization whose mission is to make the connected world a safer place by developing, validating, and promoting timely best practice solutions that help people, businesses, and governments protect themselves against pervasive cyber threats.

For additional information, visit www.cisecurity.org.

Contents

Acronyms

ACL	Access Control List
CIFS	Common Internet File System
CIS	Center for Internet Security
IT	Information Technology
COVID-19	Coronavirus Disease 2019
L1	Level 1 CIS Benchmark
MFA	Multi-Factor Authentication
NetBIOS	Network Basic Input/Output System
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
OS	Operating System
RDG	Remote Desktop Gateway
RDP	Remote Desktop Protocol
SDDC	Software Defined Data Center
SMB	Server Message Block
SPN	Service Principal Name
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network

Overview

Introduction

The CIS Critical Security Controls® (CIS Controls®) are a prioritized set of actions which collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. They are developed by a community of information technology (IT) experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors including retail, manufacturing, healthcare, education, government, defense, and others. While the CIS Controls address the general practices that most enterprises should take to secure their systems, some operational environments may present unique requirements not addressed by the CIS Controls.

We are at a point in cybersecurity where offense must inform defense in order to help protect against the most prolific cyber threats to our environments. Attacks using exploited protocols have been, and continue to be, on the rise. While attacks on exploited protocols have been happening for years before the COVID-19 pandemic, they have been of particular interest during the pandemic due to the massive shift in telecommuting. One of the more common exploited protocols, Server Message Block, or SMB, is a network file-sharing protocol that is used for a variety of purposes, which will be discussed in detail later in this guide. While some of these exploits occur due to vulnerabilities within the SMB protocol, others may occur as a result of enterprises failing to implement best practices surrounding SMB.

The purpose of this guide is to focus on direct mitigations for SMB, as well as which best practices an enterprise can put in place to reduce the risk of an SMB-related attack. We'll discuss various defensive approaches to deliver a set of best practices that all enterprises can use, in part or whole, to protect against attacks exploiting this protocol.

Purpose

SMB is a proprietary Microsoft® Windows communication protocol that is most notably used for file and printer sharing. Typically, SMB runs on port 445 (Transmission Control Protocol/Internet Protocol (TCP/IP)). SMB may also run on port 139 (Network Basic Input/Output System (NetBIOS) over TCP/IP), although this type of communication is generally only used in legacy applications and systems. There have been many versions of SMB throughout the years, including SMB v1.0/CIFS (Common Internet File System), SMB 2.0, all the way up to the most recent version, SMB 3.1.1. A similar protocol to SMB, named Samba, is used in Unix® and macOS® operating systems. Microsoft formally defines SMB as:

> **"The Server Message Block (SMB) protocol is a network file sharing protocol that allows applications on a computer to read and write to files and to request services from server programs in a computer network. The SMB protocol can be used on top of its TCP/IP protocol or other network protocols. Using the SMB protocol, an application (or the user of an application) can access files or other resources at a remote server. This allows applications to read, create, and update files on the remote server.**

SMB can also communicate with any server program that is set up to receive an SMB client request. SMB is a fabric protocol that is used by Software-defined Data Center (SDDC) computing technologies, such as Storage Spaces Direct, Storage Replica. For more information, see Windows Server software-defined datacenter." (Microsoft, 2020)

According to open-source intelligence, an estimated 1.2 million systems have SMB exposed to the public internet, many of which are still using SMB v1.0. This does not necessarily mean that 1.2 million systems are being successfully exploited. However, it does mean that the surface area for an SMB attack is expansive. SMB still remains a top attacked protocol, among others, such as Remote Desktop Protocol (RDP)[1]. When systems become internet-connected, it is inevitable that attackers will seek to exploit them in some way. As many enterprises use SMB in their day-to-day business functions, it is important to understand how to secure it.

The purpose of this guide is to provide an overview of what SMB is, some attacks associated with this protocol, and direct mitigations that an enterprise can implement to protect SMB and, ultimately, defend against an SMB-based attack.

Benefits of SMB

SMB has many benefits, including:

- Ease of having files in a central location for multiple users to access. This can be particularly helpful for end-users who may work from home or various remote locations and need access to files maintained or managed by themselves or others. It also reduces the need for activities, such as emailing or downloading files to removable media, which can increase the risk of disclosing sensitive or proprietary data should a compromise occur.
- Provides centralized control, so that systems administrators are able to control access to the files and shares at the user or group level. This, in turn, makes it easy for provisioning and deprovisioning accounts. Additionally, enterprises can set up centralized logging and monitoring, which can help with incident response, should an incident occur.
- Other benefits, introduced in SMB v3.0 and up, include end-to-end encryption, continuous availability of server applications, such as Hyper-V and Microsoft SQL Server, and pre-authentication integrity checks (SMB v3.1.1), for added security.

Attacks Using SMB

If there is one thing that remains constant over the years, it is that if the opportunity arises, attackers will aim for low-hanging fruit to exploit a system, as opposed to using complex attack techniques. SMB vulnerabilities have been around for over 20 years, with the earliest documented vulnerability recorded in 1999. Perhaps the most prolific vulnerability was disclosed on March 14, 2017, when Microsoft released its Security Bulletin (MS17-010), notifying of a critical vulnerability in SMB v1.0 that could allow for remote code execution. One month later, the exploit code was released by a hacking group called the ShadowBrokers and dubbed the EternalBlue exploit. What the world was not prepared for was that this exploit would set the stage for a whole new variety of threats that would impact us to this very day.

[1] Recently, CIS published the guide Exploited Protocols: Remote Desktop Protocol (RDP), which can be found here: https://www.cisecurity.org/blog/commonly-exploited-protocols-remote-desktop-protocol-rdp/

The first of these threats occurred in May of 2017, when a ransomware variant, named WannaCry, impacted hundreds of thousands of systems globally across all different sectors. Ransomware, a type of malware that blocks access to a device until a ransom is paid, continues to be a top threat even into 2021. One of the reasons that WannaCry was able to compromise so many systems is due to the use of the EternalBlue exploit. EternalBlue exploits a vulnerability in SMB v1.0 that allows cyber threat actors to remotely execute arbitrary code and gain access to a network by sending specially crafted packets. Fortunately, WannaCry infections drastically decreased quickly after a security researcher found a way to activate the kill switch that was built into WannaCry's code. Shortly after, a larger threat emerged that also used the EternalBlue exploit, named Emotet.

Emotet, which started out as a banking Trojan in 2014, became a self-propagating malware in 2017, shortly after the EternalBlue exploit was released. Emotet has multiple spreader modules, one of which utilizes the EternalBlue exploit, allowing the malware to spread quickly throughout a network. While Emotet is primarily disseminated through MalSpam (emails containing malicious attachments or links), it has most recently been seen in combination with ransomware infections, where an attacker will exploit a system with Emotet first, followed by deploying ransomware. After years of infecting systems, Emotet's reign ended in January 2021. TrickBot, another self-propagating malware first seen in 2016 that has various spreader modules, also exploits the SMB protocol to spread laterally throughout a network, and is prevalent still to this day.

While some of these threats may no longer be relevant present day, it is important to note that as new threats emerge, they will continue to use similar attack techniques to exploit a system or network. The recent SolarWinds attack is a good example of this, as it too exploited the SMB protocol.

How to Use This Guide

This guide is intended to assist enterprises that would like to implement the use of SMB, and are not sure where to start, or want to know how to best secure SMB if already in use by an enterprise. CIS has combined mitigations and best practices from CIS Controls and CIS Benchmarks™ to deliver a singular document that enterprises can use to secure SMB with confidence.

Each section provides a high-level overview of the direct mitigation for securing SMB, followed by the applicable CIS Controls and/or CIS Benchmarks. CIS Controls include, and are ordered by their respective mapping to the National Institute of Standards and Technology Cybersecurity Framework (NIST® CSF).

In addition to direct mitigations, supportive CIS Safeguards for protecting against an SMB-based attack are included in Appendix A of this guide. A full listing of all applicable CIS Safeguards and Benchmarks can be found in Appendices B and C of this document, respectively.

Direct Mitigations for Securing SMB

Overall, there are several direct mitigations for securing SMB, many of which are low cost or no cost to an enterprise:

- Update and Patch Against SMB Vulnerabilities
- Block SMB at the Network Level
- Restrict and Protect SMB at the Host Level
- Use Secure Authentication Methods for SMB
- Enable Encryption for SMB

Discussed below are direct mitigations that can be put in place to lock down SMB, why they are important from an attack perspective, and how the mitigations can be implemented.

Update and Patch Against SMB Vulnerabilities

Why is this important?

As with the exploits that were described above, including WannaCry and Emotet, one of the many recommendations suggested by MS17-010 was, and still is, to disable SMB v1.0. At the time, the recommendation was to update to SMB v2.0 or 3.0. However, SMB's most recent version is now SMB v3.1.1. Despite using the latest version of SMB, it is also important to keep operating systems and software up-to-date that use the SMB protocol, to ensure that any known vulnerabilities are addressed before an exploit can occur. A perfect example of this is CVE-2020-0796, also known as SMBGhost—a remote code execution vulnerability in the SMB v3.1.1 protocol.

How can this be implemented?

Deploying automated operating system and software patch management ensures that the latest security updates are applied. The CIS Microsoft Windows 10 Benchmarks have several recommendations for enabling automated patching, as well as how to disable SMB v1.0, as shown in the list directly below. Patching must also be timely, as demonstrated with the immediate exploit of vulnerabilities released in MS17-010. For servers and other business-critical systems, patches should first be applied in a testing environment, when possible, to ensure they will not negatively impact business operations in production systems. It is also important to recognize that some legacy systems and applications can only operate with SMB v1.0. In the event that an enterprise faces this issue, having mitigating controls in place, such as not exposing those systems with SMB v1.0 enabled to the internet and implementing least privilege, where possible, is recommended.

Related CIS Safeguards

- **2.2 –** Ensure Authorized Software is Currently Supported (Identify)
- **7.1 –** Establish and Maintain a Vulnerability Management Process (Protect)
- **7.2 –** Establish and Maintain a Remediation Process (Respond)
- **7.3 –** Perform Automated Operating System Patch Management (Protect)
- **7.4 –** Perform Automated Application Patch Management (Protect)
- **12.1 –** Ensure Network Infrastructure is Up-to-Date (Protect)
- **14.7 –** Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates (Protect)
- **7.7 –** Remediate Detected Vulnerabilities (Respond)

Related CIS Microsoft Windows 10 Enterprise Release 20H2 Benchmark v1.10.0

- **18.9.102.2 –** (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled'
- **18.9.102.3 –** (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'
- **18.9.102.4 –** (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'
- **18.9.102.5 –** (L1) Ensure 'Remove access to "Pause updates" feature' is set to 'Enabled'
- **18.3.2 –** (L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)'
- **18.3.3 –** (L1) Ensure 'Configure SMB v1 server' is set to 'Disabled'

Block SMB at the Network Level

Why is this important?

Attackers continuously scan for open (and potentially vulnerable) ports, such as SMB, that are connected to the internet. This is why it is important that systems using SMB are not directly exposed to the public internet. Having such systems open can not only result in a compromise of the system exposed externally, but also a potential compromise of the entire network, including internal systems.

How can this be implemented?

Rather than directly exposing SMB-enabled systems to the internet, consider putting these systems behind a Virtual Private Network (VPN) or Remote Desktop Gateway (RDG) where controls, such as multi-factor authentication (MFA), can be implemented on the endpoint for enhanced security. If an enterprise is unable to utilize an RDG or VPN, firewall rules at the network layer can help to control or block SMB traffic. This can be achieved by blocking all versions of SMB at the network layer for ports TCP/445, TCP/139, and User Datagram Protocol (UDP)/137-138, inbound and outbound. It is important to note that if an attacker is already in an enterprise's network, this mitigation will not protect them from moving around laterally within the network. This mitigation will only protect an enterprise from an attacker compromising an internet-connected system through the SMB protocol. Performing regular, automated port scans and vulnerability scans will help to easily detect systems that may have SMB directly exposed to the internet.

Related CIS Safeguards

- **5.5** – Establish and Maintain an Inventory of Service Accounts (Identify)
- **7.5 –** Perform Automated Vulnerability Scans of Internal Enterprise Assets (Identify)
- **7.6 –** Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets (Identify)
- **4.1 –** Establish and Maintain a Secure Configuration Process (Protect)
- **4.2 –** Establish and Maintain a Secure Configuration Process for Network Infrastructure (Protect)
- **4.4 –** Implement and Manage a Firewall on Servers (Protect)
- **4.5 –** Implement and Manage a Firewall on End-User Devices (Protect)
- **4.8 –** Uninstall or Disable Unnecessary Services on Enterprise Assets and Software (Protect)
- **6.4 –** Require MFA for Remote Network Access (Protect)
- **6.5 –** Require MFA for Administrative Access (Protect)
- **7.1 –** Establish and Maintain a Vulnerability Management Process (Protect)
- **7.2 –** Establish and Maintain a Remediation Process (Respond)
- **13.5 –** Manage Access Control for Remote Assets (Protect)
- **13.8 –** Deploy a Network Intrusion Prevention Solution (Protect)
- **13.3 –** Deploy a Network Intrusion Detection Solution (Detect)
- **7.7 –** Remediate Detected Vulnerabilities (Respond)

Restrict and Protect SMB at the Host Level

Why is this important?

While it is important to harden access at the network layer, it is equally important to restrict and protect access at the host level, especially for a protocol such as SMB. Long ago, before file shares and domain controllers existed, hosts may have had a reason to utilize workstation-to-workstation communication via SMB. This meant that SMB-enabled System A could communicate with SMB-enabled System B to perform various functions, such as sharing a file. Many enterprises today have dedicated file and print servers, eliminating the need for workstation-to-workstation communication. However, this type of communication can still occur with administrator-level accounts through what Windows calls "hidden shares" (IPC$, ADMIN$, and C$, to name a few). Unfortunately, while this type of communication can be used by legitimate administrators, it can also be used by attackers to move laterally throughout a network.

Having inbound host communication with file shares and domain controllers (another system that utilizes SMB) is perfectly fine, as long as an enterprise is using an up-to-date version of SMB. In fact, many of the services on those business-critical systems wouldn't function without the use of SMB. However, there should be very little business need for workstations to communicate directly with one another at the host level. These types of weaknesses can allow for attackers and self-propagating malware to spread laterally within a network, and quickly.

How can this be implemented?

To restrict SMB at the host level, use Group Policy to set up a Windows Defender Firewall rule to restrict inbound SMB communication between hosts. If administrative access via SMB is needed by administrators, configure the firewall to allow inbound SMB connections from only specific, trusted hosts. Starting with Windows 10, inbound SMB connections are now disabled by default.

Outbound communication to file servers and domain controllers within an enterprise's network is perfectly fine, as long as an up-to-date version of SMB is being used. However, since Windows Defender Firewall allows any outbound SMB connections (including public IPs), for added security, an enterprise can block outbound SMB traffic originating from public IP addresses on ports TCP/445, TCP/139, and UDP/137-138.

Related CIS Safeguards

- **7.5 –** Perform Automated Vulnerability Scans of Internal Enterprise Assets (Identify)
- **4.1 –** Establish and Maintain a Secure Configuration Process (Protect)
- **4.4 –** Implement and Manage a Firewall on Servers (Protect)
- **4.5 –** Implement and Manage a Firewall on End-User Devices (Protect)
- **7.1 –** Establish and Maintain a Vulnerability Management Process (Protect)
- **7.2 –** Establish and Maintain a Remediation Process (Respond)
- **7.7 –** Remediate Detected Vulnerabilities (Respond)

Use Secure Authentication Methods for SMB

Why is this important?

Secure authentication for SMB is important, especially when protecting against unauthorized access to sensitive data on file shares. SMB uses user-level authentication, meaning that a user must provide a username and password when requesting access to a share. From there, the user will have access to all of the shares as long as it is not restricted by share-level security. Share-level security is set by an administrator, who can assign permissions at a user or group level. Shares protected by share-level security require different credentials that are used for that share only; however, no username is required to authenticate.

How can this be implemented?

While SMB using user-level authentication does not require a separate username or password to authenticate, it does use the host credentials to authenticate, which is why it is important to use unique and complex passwords for host-based systems using SMB. Recently, CIS published a Password Policy Guide using guidance from both NIST and Microsoft to provide best practices when it comes to authentication. Additionally, the CIS Microsoft Windows 10 Benchmarks offer best practices for creating secure user credentials on the host, as shown below (CIS Microsoft Windows 10 Benchmarks 18.9.62.3.9.1, 18.9.62.2.2, and 1.1.1 – 1.1.7).

There are also additional configurations that can be implemented for hardening SMB authentication, including ensuring 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher. This will control the level of validation a server performs on the service principal name (SPN) when establishing a session using SMB. By enabling this setting, it reduces the risk of an attacker spoofing a computer to gain unauthorized access to network resources, often referred to as an SMB relay attack. Additionally, ensuring 'Accounts: Guest account status' is set to 'Disabled' will require all network users to authenticate before they can access shared resources. SMB also offers a security mechanism called SMB Signing, which digitally signs SMB packets to help improve the security of SMB. Enabling SMB packet signing (shown below as 'Digitally sign communications') reduces the risk of SMB session hijacking, which allows an attacker to interrupt, end, or steal a session that is in progress. By not enabling SMB packet signing, an enterprise increases the risk of an attacker modifying the packet to perform adverse actions or gain access to sensitive data.

Related CIS Safeguards

- **3.10 –** Encrypt Sensitive Data in Transit (Protect)
- **4.1 –** Establish and Maintain a Secure Configuration Process (Protect)
- **4.3 –** Configure Automatic Session Locking on Enterprise Assets (Protect)
- **4.7 –** Manage Default Accounts on Enterprise Assets and Software (Protect)
- **5.2 –** Use Unique Passwords (Protect)
- **5.4 –** Restrict Administrator Privileges to Dedicated Administrator Accounts (Protect)
- **5.3 –** Disable Dormant Accounts (Respond)

Related CIS Microsoft Windows 10 Enterprise Release 20H2 Benchmark v1.10.0

- **2.3.8.3 –** (L1) Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled'
- **18.5.8.1 –** (L1) Ensure 'Enable insecure guest logons' is set to 'Disabled'
- **2.3.1.3 –** (L1) Ensure 'Accounts: Guest account status' is set to 'Disabled'
- **2.2.2 –** (L1) Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users'
- **18.5.14.1 –** (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'
- **5.3 –** (L1) Ensure 'Computer Browser (Browser)' is set to 'Disabled' or 'Not Installed'
- **2.3.8.1 –** (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'

- **2.3.8.2 –** (L1) Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled'
- **2.3.9.2 –** (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'
- **2.3.9.3 –** (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'
- **2.3.9.5 –** (L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher.
- **2.3.9.1 –** (L1) Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)'
- **2.3.9.4 –** (L1) Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled'
- **2.3.11.6 –** (L1) Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled'
- **18.9.62.3.9.1 –** (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'
- **18.9.62.2.2 –** (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled'
- **1.1.1 –** (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'
- **1.1.2 –** (L1) Ensure 'Maximum password age' is set to '60 or fewer days, but not 0'
- **1.1.3 –** (L1) Ensure 'Minimum password age' is set to '1 or more day(s)'
- **1.1.4 –** (L1) Ensure 'Minimum password length' is set to '14 or more character(s)'
- **1.1.5 –** (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled'
- **1.1.6 –** (L1) Ensure 'Relax minimum password length limits' is set to 'Enabled'
- **1.1.7 –** (L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled'

Enable Encryption for SMB

Why is this important?

For enterprises that want, or are required, to encrypt file shares or entire servers, SMB v3.0 and up now offers end-to-end encryption, using AES-128-CCM (Advanced Encryption Standard-128-Cipher block chaining - message authentication code). The most recent version, SMB v3.1.1, offers AES-128-GCM (AES-128-Galois/Counter Mode) as an encryption option, as well as pre-authentication integrity checks, for added security.

How can this be implemented?

It is important to note that SMB only protects data in transit, and is actually a more cost-effective method for protecting data, as compared to other, more expensive alternatives. SMB encryption is not enabled by default in a Windows environment. For step-by-step instructions on how to enable SMB encryption, more information can be found here. While enabling encryption in transit will help protect against an SMB-related attack, it should be noted that encryption can also impact system performance.

Related CIS Safeguards

- **3.10 –** Encrypt Sensitive Data in Transit (Protect)

Conclusion

In general, most cyber-attacks involving SMB do not occur because an enterprise failed to procure an expensive tool or application, but rather because there was a failure to implement the appropriate best practices. By implementing these direct mitigations and supporting safeguards using the CIS Controls and CIS Benchmarks, an enterprise can confidently strengthen their cybersecurity posture to help protect and defend against an SMB-based attack.

References and Resources

- **Overview of file sharing using the SMB 3 protocol in Windows Server:** https://docs.microsoft.com/en-us/windows-server/storage/file-server/file-server-smb-overview
- **Microsoft Security Bulletin MS17-010:** https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010
- **CIS Password Policy Guide:** https://www.cisecurity.org/white-papers/cis-password-policy-guide/
- **SMB security enhancements:** https://docs.microsoft.com/en-us/windows-server/storage/file-server/smb-security
- **CIS Hardware and Software Asset Tracking Spreadsheet:** https://www.cisecurity.org/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet/
- **The 18 CIS Controls:** https://www.cisecurity.org/controls/cis-controls-list/
- **CIS Benchmarks:** https://www.cisecurity.org/cis-benchmarks/
- **Commonly Exploited Protocols: Remote Desktop Protocol (RDP):** https://www.cisecurity.org/blog/commonly-exploited-protocols-remote-desktop-protocol-rdp/

APPENDIX A

Supportive Safeguards for Protecting Against an SMB-Based Attack

There are a number of supportive controls that can be implemented to protect against an SMB-based attack.

- Keep Inventory and Control of Enterprise Assets That Use SMB
- Protect Data
- Perform Network Segmentation for Administrators Using SMB
- Log and Monitor for SMB-Related Events

Each supportive control will be discussed in detail below.

Keep Inventory and Control of Enterprise Assets That Use SMB

Why is this important?

Knowing which systems do and do not have SMB enabled is the first step in preparing to defend against an SMB-based attack. Arguably the most foundational of all controls, keeping inventory and control of enterprise assets, is important because you cannot protect an asset if you don't know it exists.

How can this be implemented?

While keeping track of inventory can be a complicated task, and one that many enterprises have difficulty implementing, there are many automated tools available to assist with this. For enterprises that do not have a formal inventory system for enterprise assets, and may be operating on a restricted budget, CIS offers a spreadsheet that can be easily used for tracking these assets, which can be found here.

Related CIS Safeguards

- **1.1 –** Establish and Maintain Detailed Enterprise Asset Inventory (Identify)
- **2.1 –** Establish and Maintain a Software Inventory (Identify)
- **2.2 –** Ensure Authorized Software is Currently Supported (Identify)
- **2.4 –** Utilize Automated Software Inventory Tools (Detect)
- **13.9 –** Deploy Port-Level Access Control (Protect)
- **1.3 –** Utilize an Active Discovery Tool (Detect)
- **1.5 –** Use a Passive Asset Discovery Tool (Detect)
- **1.2 –** Address Unauthorized Assets (Respond)
- **2.3 –** Address Unauthorized Software (Respond)

Protect Data

Why is this important?

Data is one of the most coveted assets that a company can have and one of the most difficult to protect. While protecting data will not mitigate an SMB-related attack, implementing these CIS Safeguards may help to reduce some of the damage that can occur during an attack.

How can this be implemented?

Ensure that data is separated by sensitivity. Back up data on a regular basis and test backups to ensure they are working properly, should they be needed in the event of an incident. Backups should also be stored securely through physical security and encryption, to prevent them from becoming destroyed or tampered with. Information should be protected through Access Control Lists (ACLs) to ensure that only authorized individuals have access to the information based on their need to know.

Related CIS Safeguards

- **3.1 –** Establish and Maintain a Data Management Process (Identify)
- **3.2 –** Establish and Maintain a Data Inventory (Identify)
- **3.7 –** Establish and Maintain a Data Classification Scheme (Identify)
- **3.8 –** Document Data Flows (Identify)
- **3.3 –** Configure Data Access Control Lists (Protect)
- **3.4 –** Enforce Data Retention (Protect)
- **3.5 –** Securely Dispose of Data (Protect)
- **3.11 –** Encrypt Sensitive Data at Rest (Protect)
- **3.12 –** Segment Data Processing and Storage Based on Sensitivity (Protect)
- **3.13 –** Deploy a Data Loss Prevention Solution (Protect)
- **11.3 –** Protect Recovery Data (Protect)
- **11.1 –** Establish and Maintain a Data Recovery Process (Recover)
- **11.2 –** Perform Automated Backups (Recover)
- **11.4 –** Establish and Maintain an Isolated Instance of Recovery Data (Recover)
- **11.5 –** Test Data Recovery (Recover)

Perform Network Segmentation for Administrators Using SMB

Why is this important?

Network segmentation is defined as separating a network into two or more subnetworks (called subnets). A network with no segmentation is generally referred to as a flat network, where all systems are on a single subnet. A flat network, while economical, can often result in more widespread damage in the event of an incident. This is an important concept because attacks exploiting SMB can spread between subnets, if not properly configured. While network segmentation in and of itself will not completely protect an enterprise from an SMB-based attack, it can increase the difficulty and possibly deter attackers or malware from causing widespread damage.

How can this be implemented?

Locking down SMB between subnets is important to reduce the risk of a network-wide compromise across multiple subnets. Administrators may sometimes use the SMB protocol between subnets to carry out their day-to-day responsibilities. If administrative access is needed between subnets, use a technology such as a jump server to carry out these administrative tasks. A jump server is a dedicated hardened system that is used to access and manage systems that have multiple subnets.

Related CIS Safeguards

- **7.5 –** Perform Automated Vulnerability Scans of Internal Enterprise Assets (Identify)
- **7.6 –** Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets (Identify)
- **12.4 –** Establish and Maintain Architecture Diagram(s) (Identify)
- **3.12 –** Segment Data Processing and Storage Based on Sensitivity (Protect)
- **7.1 –** Establish and Maintain a Vulnerability Management Process (Protect)
- **7.2 –** Establish and Maintain a Remediation Process (Protect)
- **12.2 –** Establish and Maintain a Secure Network Architecture (Protect)
- **7.7 –** Remediate Detected Vulnerabilities (Respond)

Log and Monitor for SMB-Related Events

Why is this important?

While having the proper preventive controls in place is important, it is equally important to have systems in place to detect an SMB-related attack, should one occur. Logging and monitoring for SMB events will help to detect when suspicious activity occurs, allowing an enterprise to investigate and determine if an attack has taken place.

How can this be implemented?

Proper configuration of logging is the first step to detecting a potential attack. As with any log file, ensure that these logs are enabled, as some may not be enabled by default. The following logs can be enabled to specifically log SMB communications within a Windows environment:

- Microsoft-Windows-SMBClient/Connectivity Event Log
- Microsoft-Windows-SMBClient/Operational Event Log
- Microsoft-Windows-SMBClient/Security Event Log
- Microsoft-Windows-SMBServer/Connectivity Event Log
- Microsoft-Windows-SMBServer/Operational Event Log
- Microsoft-Windows-SMBServer/Security Event Log

Related CIS Safeguards

- **8.1 –** Establish and Maintain an Audit Log Management Process (Protect)
- **8.4 –** Standardize Time Synchronization (Protect)
- **8.3 –** Ensure Adequate Audit Log Storage (Protect)
- **8.10 –** Retain Audit Logs (Protect)
- **3.14 –** Log Sensitive Data Access (Detect)
- **8.2 –** Collect Audit Logs (Detect)
- **8.5 –** Collect Detailed Audit Logs (Detect)
- **8.9 –** Centralize Audit Logs (Detect)
- **8.11 –** Conduct Audit Log Reviews (Detect)
- **13.1 –** Centralize Security Event Alerting (Detect)
- **13.6 –** Collect Network Traffic Flow Logs (Detect)
- **13.11 –** Tune Security Event Alerting Thresholds (Detect)

APPENDIX B

CIS Controls

Implementation Groups

In CIS Controls v8, we created Implementation Groups (IGs) to provide granularity and some explicit structure to the different realities faced by enterprises of varied sizes.

IG1

An IG1 enterprise is small to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. The principal concern of these enterprises is to keep the business operational as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and principally involves employee and financial information. However, there may be some small to medium-sized enterprises that are responsible for protecting sensitive data and, therefore, will fall into a higher group. Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office commercial-off-the-shelf (COTS) hardware and software.

IG2

An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with different risk profiles based on job function and mission. Small organizational units may have regular compliance burdens. Implementation Group 2 enterprises often store and process sensitive client or company information and can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs. Safeguards selected for IG2 help security teams cope with increased operational complexity. Some Safeguards will depend on enterprise-grade technology and specialized expertise to properly install and configure.

IG3

An IG3 enterprise employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 systems and data contain sensitive information or functions that are subject to regulatory and compliance oversight. An IG3 enterprise must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare. Safeguards selected for IG3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

To learn more about the Implementation Groups within the CIS Controls and how they pertain to enterprises of all sizes, visit our website at https://www.cisecurity.org/controls/cis-controls-list/.

SMB-Related Recommendations

Below is a list of CIS Safeguards associated with securing SMB.

CONTROL	SAFEGUARD	TITLE	ASSET TYPE	NIST SECURITY FUNCTION	IG1	IG2	IG3	SMB-RELATED RECOMMENDATION	DIRECT MITIGATION OR SUPPORTIVE SAFEGUARD?
2	2.2	Ensure Authorized Software is Currently Supported	Applications	Identify	●	●	●	Update and Patch Against SMB Vulnerabilities	Direct Mitigation
7	7.1	Establish and Maintain a Vulnerability Management Process	Applications	Protect	●	●	●	Update and Patch Against SMB Vulnerabilities	Direct Mitigation
7	7.2	Establish and Maintain a Remediation Process	Applications	Respond	●	●	●	Update and Patch Against SMB Vulnerabilities	Direct Mitigation
7	7.3	Perform Automated Operating System Patch Management	Applications	Protect	●	●	●	Update and Patch Against SMB Vulnerabilities	Direct Mitigation
7	7.4	Perform Automated Application Patch Management	Applications	Protect	●	●	●	Update and Patch Against SMB Vulnerabilities	Direct Mitigation
12	12.1	Ensure Network Infrastructure is Up-to-Date	Network	Protect	●	●	●	Update and Patch Against SMB Vulnerabilities	Direct Mitigation
14	14.7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	N/A	Protect	●	●	●	Update and Patch Against SMB Vulnerabilities	Direct Mitigation
7	7.7	Remediate Detected Vulnerabilities	Applications	Respond		●	●	Update and Patch Against SMB Vulnerabilities	Direct Mitigation
5	5.5	Establish and Maintain an Inventory of Service Accounts	Users	Identify		●	●	Block SMB at the Network Level	Direct Mitigation
7	7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets	Applications	Identify		●	●	Block SMB at the Network Level	Direct Mitigation
7	7.6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	Applications	Identify		●	●	Block SMB at the Network Level	Direct Mitigation
4	4.1	Establish and Maintain a Secure Configuration Process	Applications	Protect	●	●	●	Block SMB at the Network Level	Direct Mitigation
4	4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Network	Protect	●	●	●	Block SMB at the Network Level	Direct Mitigation
4	4.4	Implement and Manage a Firewall on Servers	Devices	Protect	●	●	●	Block SMB at the Network Level	Direct Mitigation
4	4.5	Implement and Manage a Firewall on End-User Devices	Devices	Protect	●	●	●	Block SMB at the Network Level	Direct Mitigation
4	4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Devices	Protect		●	●	Block SMB at the Network Level	Direct Mitigation
6	6.4	Require MFA for Remote Network Access	Users	Protect	●	●	●	Block SMB at the Network Level	Direct Mitigation
6	6.5	Require MFA for Administrative Access	Users	Protect	●	●	●	Block SMB at the Network Level	Direct Mitigation
7	7.1	Establish and Maintain a Vulnerability Management Process	Applications	Protect	●	●	●	Block SMB at the Network Level	Direct Mitigation

CONTROL	SAFEGUARD	TITLE	ASSET TYPE	NIST SECURITY FUNCTION	IG1	IG2	IG3	SMB-RELATED RECOMMENDATION	DIRECT MITIGATION OR SUPPORTIVE SAFEGUARD?
7	7.2	Establish and Maintain a Remediation Process	Applications	Respond	●	●	●	Block SMB at the Network Level	Direct Mitigation
13	13.5	Manage Access Control for Remote Assets	Devices	Protect		●	●	Block SMB at the Network Level	Direct Mitigation
13	13.8	Deploy a Network Intrusion Prevention Solution	Network	Protect			●	Block SMB at the Network Level	Direct Mitigation
13	13.3	Deploy a Network Intrusion Detection Solution	Network	Detect		●	●	Block SMB at the Network Level	Direct Mitigation
7	7.7	Remediate Detected Vulnerabilities	Applications	Respond		●	●	Block SMB at the Network Level	Direct Mitigation
7	7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets	Applications	Identify		●	●	Restrict and Protect SMB at the Host Level	Direct Mitigation
4	4.1	Establish and Maintain a Secure Configuration Process	Applications	Protect	●	●	●	Restrict and Protect SMB at the Host Level	Direct Mitigation
4	4.4	Implement and Manage a Firewall on Servers	Devices	Protect	●	●	●	Restrict and Protect SMB at the Host Level	Direct Mitigation
4	4.5	Implement and Manage a Firewall on End-User Devices	Devices	Protect	●	●	●	Restrict and Protect SMB at the Host Level	Direct Mitigation
7	7.1	Establish and Maintain a Vulnerability Management Process	Applications	Protect	●	●	●	Restrict and Protect SMB at the Host Level	Direct Mitigation
7	7.2	Establish and Maintain a Remediation Process	Applications	Respond	●	●	●	Restrict and -Protect- SMB at the Host Level	Direct Mitigation
7	7.7	Remediate Detected Vulnerabilities	Applications	Respond		●	●	Restrict and Protect SMB at the Host Level	Direct Mitigation
3	3.10	Encrypt Sensitive Data in Transit	Data	Protect		●	●	Use Secure Authentication Methods for SMB	Direct Mitigation
4	4.1	Establish and Maintain a Secure Configuration Process	Applications	Protect	●	●	●	Use Secure Authentication Methods for SMB	Direct Mitigation
4	4.3	Configure Automatic Session Locking on Enterprise Assets	Users	Protect	●	●	●	Use Secure Authentication Methods for SMB	Direct Mitigation
4	4.7	Manage Default Accounts on Enterprise Assets and Software	Users	Protect	●	●	●	Use Secure Authentication Methods for SMB	Direct Mitigation
5	5.2	Use Unique Passwords	Users	Protect	●	●	●	Use Secure Authentication Methods for SMB	Direct Mitigation
5	5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	Users	Protect	●	●	●	Use Secure Authentication Methods for SMB	Direct Mitigation
5	5.3	Disable Dormant Accounts	Users	Respond	●	●	●	Use Secure Authentication Methods for SMB	Direct Mitigation
3	3.10	Encrypt Sensitive Data in Transit	Data	Protect		●	●	Enable Encryption for SMB	Direct Mitigation
1	1.1	Establish and Maintain Detailed Enterprise Asset Inventory	Devices	Identify	●	●	●	Keep Inventory and Control of Enterprise Assets That Use SMB	Supportive Safeguard
2	2.1	Establish and Maintain a Software Inventory	Applications	Identify	●	●	●	Keep Inventory and Control of Enterprise Assets That Use SMB	Supportive Safeguard

CONTROL	SAFEGUARD	TITLE	ASSET TYPE	NIST SECURITY FUNCTION	IG1	IG2	IG3	SMB-RELATED RECOMMENDATION	DIRECT MITIGATION OR SUPPORTIVE SAFEGUARD?
2	2.2	Ensure Authorized Software is Currently Supported	Applications	Identify	●	●	●	Keep Inventory and Control of Enterprise Assets That Use SMB	Supportive Safeguard
2	2.4	Utilize Automated Software Inventory Tools	Applications	Detect		●	●	Keep Inventory and Control of Enterprise Assets That Use SMB	Supportive Safeguard
13	13.9	Deploy Port-Level Access Control	Devices	Protect			●	Keep Inventory and Control of Enterprise Assets That Use SMB	Supportive Safeguard
1	1.3	Utilize an Active Discovery Tool	Devices	Detect		●	●	Keep Inventory and Control of Enterprise Assets That Use SMB	Supportive Safeguard
1	1.5	Use a Passive Asset Discovery Tool	Devices	Detect			●	Keep Inventory and Control of Enterprise Assets That Use SMB	Supportive Safeguard
1	1.2	Address Unauthorized Assets	Devices	Respond	●	●	●	Keep Inventory and Control of Enterprise Assets That Use SMB	Supportive Safeguard
2	2.3	Address Unauthorized Software	Applications	Respond	●	●	●	Keep Inventory and Control of Enterprise Assets That Use SMB	Supportive Safeguard
3	3.1	Establish and Maintain a Data Management Process	Data	Identify	●	●	●	Protect Data	Supportive Safeguard
3	3.2	Establish and Maintain a Data Inventory	Data	Identify	●	●	●	Protect Data	Supportive Safeguard
3	3.7	Establish and Maintain a Data Classification Scheme	Data	Identify		●	●	Protect Data	Supportive Safeguard
3	3.8	Document Data Flows	Data	Identify		●	●	Protect Data	Supportive Safeguard
3	3.3	Configure Data Access Control Lists	Data	Protect	●	●	●	Protect Data	Supportive Safeguard
3	3.4	Enforce Data Retention	Data	Protect		●	●	Protect Data	Supportive Safeguard
3	3.5	Securely Dispose of Data	Data	Protect	●	●	●	Protect Data	Supportive Safeguard
3	3.11	Encrypt Sensitive Data at Rest	Data	Protect		●	●	Protect Data	Supportive Safeguard
3	3.12	Segment Data Processing and Storage Based on Sensitivity	Network	Protect		●	●	Protect Data	Supportive Safeguard
3	3.13	Deploy a Data Loss Prevention Solution	Data	Protect			●	Protect Data	Supportive Safeguard
11	11.3	Protect Recovery Data	Data	Protect	●	●	●	Protect Data	Supportive Safeguard
11	11.1	Establish and Maintain a Data Recovery Process	Data	Recover	●	●	●	Protect Data	Supportive Safeguard
11	11.2	Perform Automated Backups	Data	Recover	●	●	●	Protect Data	Supportive Safeguard
11	11.4	Establish and Maintain an Isolated Instance of Recovery Data	Data	Recover	●	●	●	Protect Data	Supportive Safeguard
11	11.5	Test Data Recovery	Data	Recover		●	●	Protect Data	Supportive Safeguard

CONTROL	SAFEGUARD	TITLE	ASSET TYPE	NIST SECURITY FUNCTION	IG1	IG2	IG3	SMB-RELATED RECOMMENDATION	DIRECT MITIGATION OR SUPPORTIVE SAFEGUARD?
7	7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets	Applications	Identify		●	●	Perform Network Segmentation for Administrators Using SMB	Supportive Safeguard
7	7.6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	Applications	Identify		●	●	Perform Network Segmentation for Administrators Using SMB	Supportive Safeguard
12	12.4	Establish and Maintain Architecture Diagram(s)	Network	Identify		●	●	Perform Network Segmentation for Administrators Using SMB	Supportive Safeguard
3	3.12	Segment Data Processing and Storage Based on Sensitivity	Network	Protect		●	●	Perform Network Segmentation for Administrators Using SMB	Supportive Safeguard
7	7.1	Establish and Maintain a Vulnerability Management Process	Applications	Protect	●	●	●	Perform Network Segmentation for Administrators Using SMB	Supportive Safeguard
7	7.2	Establish and Maintain a Remediation Process	Applications	Respond	●	●	●	Perform Network Segmentation for Administrators Using SMB	Supportive Safeguard
12	12.2	Establish and Maintain a Secure Network Architecture	Network	Protect		●	●	Perform Network Segmentation for Administrators Using SMB	Supportive Safeguard
7	7.7	Remediate Detected Vulnerabilities	Applications	Respond		●	●	Perform Network Segmentation for Administrators Using SMB	Supportive Safeguard
8	8.1	Establish and Maintain an Audit Log Management Process	Network	Protect	●	●	●	Log and Monitor for SMB-Related Events	Supportive Safeguard
8	8.4	Standardize Time Synchronization	Network	Protect		●	●	Log and Monitor for SMB-Related Events	Supportive Safeguard
8	8.3	Ensure Adequate Audit Log Storage	Network	Protect	●	●	●	Log and Monitor for SMB-Related Events	Supportive Safeguard
8	8.10	Retain Audit Logs	Network	Protect		●	●	Log and Monitor for SMB-Related Events	Supportive Safeguard
3	3.14	Log Sensitive Data Access	Data	Detect			●	Log and Monitor for SMB-Related Events	Supportive Safeguard
8	8.2	Collect Audit Logs	Network	Detect	●	●	●	Log and Monitor for SMB-Related Events	Supportive Safeguard
8	8.5	Collect Detailed Audit Logs	Network	Detect		●	●	Log and Monitor for SMB-Related Events	Supportive Safeguard
8	8.9	Centralize Audit Logs	Network	Detect		●	●	Log and Monitor for SMB-Related Events	Supportive Safeguard
8	8.11	Conduct Audit Log Reviews	Network	Detect		●	●	Log and Monitor for SMB-Related Events	Supportive Safeguard
13	13.1	Centralize Security Event Alerting	Network	Detect		●	●	Log and Monitor for SMB-Related Events	Supportive Safeguard
13	13.6	Collect Network Traffic Flow Logs	Network	Detect		●	●	Log and Monitor for SMB-Related Events	Supportive Safeguard
13	13.11	Tune Security Event Alerting Thresholds	Network	Detect			●	Log and Monitor for SMB-Related Events	Supportive Safeguard

APPENDIX C

CIS Benchmarks

SMB-Related Recommendations

Below is a list of CIS Benchmarks, from the CIS Microsoft Windows 10 Enterprise Release 20H2 Benchmark v1.10.0, associated with securing SMB. Note that each Benchmark is designated with an L1. The Level 1 profile is considered a base recommendation that can be implemented fairly promptly and is designed to not have an extensive performance impact. The intent of the Level 1 profile CIS Benchmark is to lower the attack surface of an enterprise while keeping machines usable and not hindering business functionality.

CIS BENCHMARK SECTION #	CIS BENCHMARK RECOMMENDATION #	CIS BENCHMARK TITLE / DESCRIPTION	SMB-RELATED RECOMMENDATION	DIRECT MITIGATION OR SUPPORTIVE CONTROL?
18.9.102	**18.9.102.2**	**(L1) Ensure 'Configure Automatic Updates' is set to 'Enabled'**	Update and Patch Against SMB Vulnerabilities	Direct Mitigation
		This policy setting specifies whether computers in your environment will receive security updates from Windows Update or WSUS. If you configure this policy setting to Enabled, the operating system will recognize when a network connection is available and then use the network connection to search Windows Update or your designated intranet site for updates that apply to them. After you configure this policy setting to Enabled, select one of the following three options in the Configure Automatic Updates Properties dialog box to specify how the service will work: • 2 - Notify for download and auto install *(Notify before downloading any updates)* • 3 - Auto download and notify for install *(Download the updates automatically and notify when they are ready to be installed.) (Default setting)* • 4 - Auto download and schedule the install *(Automatically download updates and install them on the schedule specified below.))* • 5 - Allow local admin to choose setting *(Leave decision on above choices up to the local Administrators (Not Recommended))* The recommended state for this setting is: **'Enabled.'** **Note:** The sub-setting "*Configure automatic updating:*" has 4 possible values – all of them are valid depending on specific organizational needs, however if feasible we suggest using a value of **'4 - Auto download and schedule the install.'** This suggestion is not a scored requirement. **Note #2:** Organizations that utilize a 3rd-party solution for patching may choose to exempt themselves from this recommendation, and instead configure it to **'Disabled'** so that the native Windows Update mechanism does not interfere with the 3rd-party patching process.		
18.9.102	**18.9.102.3**	**(L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'**	Update and Patch Against SMB Vulnerabilities	Direct Mitigation
		This policy setting specifies when computers in your environment will receive security updates from Windows Update or WSUS. The recommended state for this setting is: **'0 - Every day.'** **Note:** This setting is only applicable if **'4 - Auto download and schedule the install'** is selected in Rule 18.9.102.2. It will have no impact if any other option is selected.		

CIS BENCHMARK SECTION #	CIS BENCHMARK RECOMMENDATION #	CIS BENCHMARK TITLE / DESCRIPTION	SMB-RELATED RECOMMENDATION	DIRECT MITIGATION OR SUPPORTIVE CONTROL?
18.9.102	**18.9.102.4**	**(L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'**	Update and Patch Against SMB Vulnerabilities	Direct Mitigation
		This policy setting specifies that Automatic Updates will wait for computers to be restarted by the users who are logged on to them to complete a scheduled installation. The recommended state for this setting is: **'Disabled.'** **Note:** This setting applies only when you configure Automatic Updates to perform scheduled update installations. If you configure the Configure Automatic Updates setting to Disabled, this setting has no effect.		
18.9.102	**18.9.102.5**	**(L1) Ensure 'Remove access to "Pause updates" feature' is set to 'Enabled'**	Update and Patch Against SMB Vulnerabilities	Direct Mitigation
		This policy removes access to "Pause updates" feature. The recommended state for this setting is: **'Enabled.'**		
18.3	**18.3.2**	**(L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)'**	Update and Patch Against SMB Vulnerabilities	Direct Mitigation
		This setting configures the start type for the Server Message Block version 1 (SMBv1) client driver service (**'MRxSmb10'**), which is recommended to be disabled. The recommended state for this setting is: **'Enabled: Disable driver (recommended)'**. **Note:** Do not, *under any circumstances*, configure this overall setting as **'Disabled'**, as doing so will delete the underlying registry entry altogether, which will cause serious problems.		
18.3	**18.3.3**	**(L1) Ensure 'Configure SMB v1 server' is set to 'Disabled'**	Update and Patch Against SMB Vulnerabilities	Direct Mitigation
		This setting configures the server-side processing of the Server Message Block version 1 (SMBv1) protocol. The recommended state for this setting is: **'Disabled'**.		
2.3.8	**2.3.8.3**	**(L1) Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled'**	Use Secure Authentication Methods for SMB	Direct Mitigation
		This policy setting determines whether the SMB redirector will send plaintext passwords during authentication to third-party SMB servers that do not support password encryption. It is recommended that you disable this policy setting unless there is a strong business case to enable it. If this policy setting is enabled, unencrypted passwords will be allowed across the network. The recommended state for this setting is: **'Disabled.'**		
18.5.8	**18.5.8.1**	**(L1) Ensure 'Enable insecure guest logons' is set to 'Disabled'**	Use Secure Authentication Methods for SMB	Direct Mitigation
		This policy setting determines if the SMB client will allow insecure guest logons to an SMB server. The recommended state for this setting is: **'Disabled.'**		

CIS BENCHMARK SECTION #	CIS BENCHMARK RECOMMENDATION #	CIS BENCHMARK TITLE / DESCRIPTION	SMB-RELATED RECOMMENDATION	DIRECT MITIGATION OR SUPPORTIVE CONTROL?
2.3.1	**2.3.1.3**	**(L1) Ensure 'Accounts: Guest account status' is set to 'Disabled'**	Use Secure Authentication Methods for SMB	Direct Mitigation
		This policy setting determines whether the Guest account is enabled or disabled. The Guest account allows unauthenticated network users to gain access to the system. The recommended state for this setting is: **'Disabled.'** **Note:** This setting will have no impact when applied to the Domain Controllers organizational unit via group policy because Domain Controllers have no local account database. It can be configured at the domain level via group policy, similar to account lockout and password policy settings.		
2.2	**2.2.2**	**(L1) Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users'**	Use Secure Authentication Methods for SMB	Direct Mitigation
		This policy setting allows other users on the network to connect to the computer and is required by various network protocols that include Server Message Block (SMB)-based protocols, NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+). The recommended state for this setting is: **'Administrators, Remote Desktop Users.'**		
18.5.14	**18.5.14.1**	**(L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'**	Use Secure Authentication Methods for SMB	Direct Mitigation
		This policy setting configures secure access to UNC paths. The recommended state for this setting is: **'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares.'** **Note:** If the environment exclusively contains Windows 8.0 / Server 2012 (non-R2) or newer systems, then the **'Privacy'** setting may (optionally) also be set to enable SMB encryption. However, using SMB encryption will render the targeted share paths completely inaccessible by older OSes, so only use this additional option with caution and thorough testing.		
5	**5.3**	**(L1) Ensure 'Computer Browser (Browser)' is set to 'Disabled' or 'Not Installed'**	Use Secure Authentication Methods for SMB	Direct Mitigation
		Maintains an updated list of computers on the network and supplies this list to computers designated as browsers. The recommended state for this setting is: **'Disabled**' or '**Not Installed.'** **Note:** In Windows 8.1 and Windows 10, this service is bundled with the *SMB 1.0/CIFS File Sharing Support* optional feature. As a result, removing that feature (highly recommended unless backward compatibility is needed to XP/2003 and older Windows OSes - see [Stop using SMB1 | Storage at Microsoft](https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/)) will also remediate this recommendation. The feature is not installed by default starting with Windows 10 R1709.		
2.3.8	**2.3.8.1**	**(L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'**	Use Secure Authentication Methods for SMB	Direct Mitigation

CIS BENCHMARK SECTION #	CIS BENCHMARK RECOMMENDATION #	CIS BENCHMARK TITLE / DESCRIPTION	SMB-RELATED RECOMMENDATION	DIRECT MITIGATION OR SUPPORTIVE CONTROL?
		This policy setting determines whether packet signing is required by the SMB client component. **Note:** When Windows Vista-based computers have this policy setting enabled and they connect to file or print shares on remote servers, it is important that the setting is synchronized with its companion setting, **Microsoft network server: Digitally sign communications (always)**, on those servers. For more information about these settings, see the "Microsoft network client and server: Digitally sign communications (four related settings)" section in Chapter 5 of the Threats and Countermeasures guide. The recommended state for this setting is: **'Enabled.'**		
2.3.8	**2.3.8.2**	**(L1) Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled'** This policy setting determines whether the SMB client will attempt to negotiate SMB packet signing. **Note:** Enabling this policy setting on SMB clients on your network makes them fully effective for packet signing with all clients and servers in your environment. The recommended state for this setting is: **'Enabled.'**	Use Secure Authentication Methods for SMB	Direct Mitigation
2.3.9	**2.3.9.2**	**(L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'** This policy setting determines whether packet signing is required by the SMB server component. Enable this policy setting in a mixed environment to prevent downstream clients from using the workstation as a network server. The recommended state for this setting is: **'Enabled.'**	Use Secure Authentication Methods for SMB	Direct Mitigation
2.3.9	**2.3.9.3**	**(L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'** This policy setting determines whether the SMB server will negotiate SMB packet signing with clients that request it. If no signing request comes from the client, a connection will be allowed without a signature if the **Microsoft network server: Digitally sign communications (always)** setting is not enabled. **Note:** Enable this policy setting on SMB clients on your network to make them fully effective for packet signing with all clients and servers in your environment. The recommended state for this setting is: **'Enabled.'**	Use Secure Authentication Methods for SMB	Direct Mitigation
2.3.9	**2.3.9.5**	**(L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher** This policy setting controls the level of validation a computer with shared folders or printers (the server) performs on the service principal name (SPN) that is provided by the client computer when it establishes a session using the server message block (SMB) protocol. The server message block (SMB) protocol provides the basis for file and print sharing and other networking operations, such as remote Windows administration. The SMB protocol supports validating the SMB server service principal name (SPN) within the authentication blob provided by a SMB client to prevent a class of attacks against SMB servers referred to as SMB relay attacks. This setting will affect both SMB1 and SMB2. The recommended state for this setting is: **'Accept if provided by client'. Configuring this setting to 'Required from client'** also conforms to the benchmark.	Use Secure Authentication Methods for SMB	Direct Mitigation

CIS BENCHMARK SECTION #	CIS BENCHMARK RECOMMENDATION #	CIS BENCHMARK TITLE / DESCRIPTION	SMB-RELATED RECOMMENDATION	DIRECT MITIGATION OR SUPPORTIVE CONTROL?
2.3.9	**2.3.9.1**	**(L1) Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)'**	Use Secure Authentication Methods for SMB	Direct Mitigation
		This policy setting allows you to specify the amount of continuous idle time that must pass in an SMB session before the session is suspended because of inactivity. Administrators can use this policy setting to control when a computer suspends an inactive SMB session. If client activity resumes, the session is automatically reestablished. The maximum value is 99999, which is over 69 days; in effect, this value disables the setting. The recommended state for this setting is: **'15 or fewer minute(s).'**		
2.3.9	**2.3.9.4**	**(L1) Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled'**	Use Secure Authentication Methods for SMB	Direct Mitigation
		This security setting determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. This setting affects the Server Message Block (SMB) component. If you enable this policy setting you should also enable *Network security: Force logoff when logon hours expire* (Rule 2.3.11.6). If your organization configures logon hours for users, this policy setting is necessary to ensure they are effective. The recommended state for this setting is: **'Enabled.'**		
2.3.11	**2.3.11.6**	**(L1) Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled'**	Use Secure Authentication Methods for SMB	Direct Mitigation
		This policy setting determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. This setting affects the Server Message Block (SMB) component. If you enable this policy setting you should also enable *Microsoft network server: Disconnect clients when logon hours expire* (Rule 2.3.9.4). The recommended state for this setting is: **'Enabled.'**		
18.9.62.3.9	**18.9.62.3.9.1**	**(L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'**	Use Secure Authentication Methods for SMB	Direct Mitigation
		This policy setting specifies whether Remote Desktop Services always prompts the client computer for a password upon connection. You can use this policy setting to enforce a password prompt for users who log on to Remote Desktop Services, even if they already provided the password in the Remote Desktop Connection client. The recommended state for this setting is: **'Enabled.'**		
18.9.62.2	**18.9.62.2.2**	**(L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled'**	Use Secure Authentication Methods for SMB	Direct Mitigation
		This policy setting helps prevent Remote Desktop clients from saving passwords on a computer. The recommended state for this setting is: **'Enabled.'** **Note:** If this policy setting was previously configured as Disabled or Not configured, any previously saved passwords will be deleted the first time a Remote Desktop client disconnects from any server.		

CIS BENCHMARK SECTION #	CIS BENCHMARK RECOMMENDATION #	CIS BENCHMARK TITLE / DESCRIPTION	SMB-RELATED RECOMMENDATION	DIRECT MITIGATION OR SUPPORTIVE CONTROL?
1.1	**1.1.1**	**(L1) Ensure 'Enforce password history' is set to '24 or more password(s)'**	Use Secure Authentication Methods for SMB	Direct Mitigation
		This policy setting determines the number of renewed, unique passwords that have to be associated with a user account before you can reuse an old password. The value for this policy setting must be between 0 and 24 passwords. The default value for Windows Vista is 0 passwords, but the default setting in a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password. The recommended state for this setting is: **'24 or more password(s).'** **Note:** Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center. **Note #2:** As of the publication of this benchmark, Microsoft currently has a maximum limit of 24 saved passwords. For more information, please visit [Enforce password history (Windows 10) - Windows security | Microsoft Docs](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/enforce-password-history#:~:text=The%20Enforce%20password%20history%20policy,a%20long%20period%20of%20time.)		
1.1	**1.1.2**	(L1) Ensure '**Maximum password age**' is set to '**60 or fewer days, but not 0'**	Use Secure Authentication Methods for SMB	Direct Mitigation
		This policy setting defines how long a user can use their password before it expires. Values for this policy setting range from 0 to 999 days. If you set the value to 0, the password will never expire. Because attackers can crack passwords, the more frequently you change the password the less opportunity an attacker has to use a cracked password. However, the lower this value is set, the higher the potential for an increase in calls to help desk support due to users having to change their password or forgetting which password is current. The recommended state for this setting is **'60 or fewer days, but not 0.'** **Note:** Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.		

CIS BENCHMARK SECTION #	CIS BENCHMARK RECOMMENDATION #	CIS BENCHMARK TITLE / DESCRIPTION	SMB-RELATED RECOMMENDATION	DIRECT MITIGATION OR SUPPORTIVE CONTROL?
1.1	**1.1.3**	**(L1) Ensure 'Minimum password age' is set to '1 or more day(s)'**	Use Secure Authentication Methods for SMB	Direct Mitigation
		This policy setting determines the number of days that you must use a password before you can change it. The range of values for this policy setting is between 1 and 999 days. (You may also set the value to 0 to allow immediate password changes.) The default value for this setting is 0 days. The recommended state for this setting is: **'1 or more day(s).'** **Note:** Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.		
1.1	**1.1.4**	**(L1) Ensure 'Minimum password length' is set to '14 or more character(s)'**	Use Secure Authentication Methods for SMB	Direct Mitigation
		This policy setting determines the least number of characters that make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps "passphrase" is a better term than "password." In Microsoft Windows 2000 and newer, passphrases can be quite long and can include spaces. Therefore, a phrase such as "I want to drink a $5 milkshake" is a valid passphrase; it is a considerably stronger password than an 8- or 10-character string of random numbers and letters, and yet is easier to remember. Users must be educated about the proper selection and maintenance of passwords, especially with regard to password length. In enterprise environments, the ideal value for the Minimum password length setting is 14 characters, however you should adjust this value to meet your organization's business requirements. The recommended state for this setting is: **'14 or more character(s).'** **Note:** In Windows Server 2016 and older versions of Windows Server, the GUI of the Local Security Policy (LSP), Local Group Policy Editor (LGPE) and Group Policy Management Editor (GPME) would not let you set this value higher than 14 characters. However, starting with Windows Server 2019, Microsoft changed the GUI to allow up to a 20-character minimum password length. **Note #2:** Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.		

CIS BENCHMARK SECTION #	CIS BENCHMARK RECOMMENDATION #	CIS BENCHMARK TITLE / DESCRIPTION	SMB-RELATED RECOMMENDATION	DIRECT MITIGATION OR SUPPORTIVE CONTROL?
1.1	**1.1.5**	**(L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled'**	Use Secure Authentication Methods for SMB	Direct Mitigation

This policy setting checks all new passwords to ensure that they meet basic requirements for strong passwords.

When this policy is enabled, passwords must meet the following minimum requirements:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least six characters in length
- Contain characters from three of the following categories:
- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, !, $, #, %)
- A catch-all category of any Unicode character that does not fall under the previous four categories. This fifth category can be regionally specific.

Each additional character in a password increases its complexity exponentially. For instance, a seven-character, all lower-case alphabetic password would have 267 (approximately 8 x 109 or 8 billion) possible combinations. At 1,000,000 attempts per second (a capability of many password-cracking utilities), it would only take 133 minutes to crack. A seven-character alphabetic password with case sensitivity has 527 combinations. A seven-character case-sensitive alphanumeric password without punctuation has 627 combinations. An eight-character password has 268 (or 2 x 1011) possible combinations. Although this might seem to be a large number, at 1,000,000 attempts per second it would take only 59 hours to try all possible passwords. Remember, these times will significantly increase for passwords that use ALT characters and other special keyboard characters such as "!" or "@." Proper use of the password settings can help make it difficult to mount a brute force attack.

The recommended state for this setting is: **'Enabled.'**

Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

1.1	**1.1.6**	**(L1) Ensure 'Relax minimum password length limits' is set to 'Enabled'**	Use Secure Authentication Methods for SMB	Direct Mitigation

This policy setting determines whether the minimum password length setting can be increased beyond the legacy limit of 14 characters. For more information please see the following [Microsoft Security Blog](https://techcommunity.microsoft.com/t5/microsoft-security-baselines/security-baseline-draft-windows-10-and-windows-server-version/ba-p/1419213).

The recommended state for this setting is: **'Enabled.'**

Note: This setting only affects *local* accounts on the computer. Domain accounts are only affected by settings on the Domain Controllers, because that is where domain accounts are stored.

CIS BENCHMARK SECTION #	CIS BENCHMARK RECOMMENDATION #	CIS BENCHMARK TITLE / DESCRIPTION	SMB-RELATED RECOMMENDATION	DIRECT MITIGATION OR SUPPORTIVE CONTROL?
1.1	**1.1.7**	**(L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled'**	Use Secure Authentication Methods for SMB	Direct Mitigation
		This policy setting determines whether the operating system stores passwords in a way that uses reversible encryption, which provides support for application protocols that require knowledge of the user's password for authentication purposes. Passwords that are stored with reversible encryption are essentially the same as plaintext versions of the passwords. The recommended state for this setting is: **'Disabled.'** **Note:** Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.		

CIS Center for Internet Security®

CIS Controls

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats.

Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.

To learn more, visit www.cisecurity.org or follow us on Twitter: @CISecurity.

cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security
@CISecurity
CenterforIntSec
TheCISecurity
cisecurity