What Is SMB Protocol ?

The Server Message Block (SMB) is an integral part of any successful organization’s technology assets. In this blog post, we’ll take an easily digestible look at SMB, including its history, why and how it is used and what SMB is used for during penetration tests.

SMB was first referenced as “IBM PC Network SMB Protocol” in a 1985 document by IBM, and in 1987 as “Microsoft Networks/OpenNet-FILE.” Each of these documents outline the very basics of SMB. Simply, SMB is a client-server protocol used to provide shared access to resources over a network which means that a client asks for files or resources and the server supplies them.

In the early years, a version of SMB was created by Microsoft and was known as Common Internet File System or CIFS. This term is still occasionally used across the internet as a synonym for SMB, but the term is antiquated. To eliminate any confusion, I use the term SMB in this blog post.

The various iterations of SMB have added functions to the protocol, and some of the high-level changes include:

* SMB 2.0 (2006)
  + Streamlined the protocol
    - The number of subcommands changed from over 100 to 19
  + Durable file handles
    - Connections to an SMB server could now survive over brief network outages
  + Backwards compatible
    - Used for communication with older versions of Windows
* SMB 2.1 (2008)
  + Opportunistic Locking
    - A form of version control, which allows a user to download a file from a share and make changes to a file, while notifying other users working on the same file that they have older versions of the file
* SMB 3.0 (2012)
  + SMB over RDMA
    - Increases the scalability and speed of storage access
    - Decreases the CPU utilization of processing
  + SMB Multichannel
    - This SMB server can transmit more data using multiple connections
* SMB 3.02 (2012)
  + SMBv1 could now be disabled
* SMB 3.1.1 (2016)
  + Implemented pre-authentication integrity check using SHA-512 hash

SMB is much like HTTP, FTP or other protocols used to get data from point A on a network to point B. There are some strengths and weaknesses, with the primary SMB strength being the ease of use. The setup across various devices on a network are seamless, so that Windows, OSX, and Linux devices can utilize SMB with little to no effort. Additionally, SMB can be used to share resources as well as files. So if a client wanted to use a printer which was connected to the SMB server, but not the client, the client could use the SMB server and connect to the printer through that server. This would also work for file systems, printers, mail slots, and APIs.

There are some drawbacks to SMB. For example, it should not be used across the internet, but only on hosts connected to the LAN. This is due to the inherent insecurity of the way SMB authenticates. Although it is still apparent on a LAN, the attack surface is greatly reduced.

In the above graphic from Microsoft, NTLM Authentication is passed when the session is set up. Although the data is encrypted, the authentication is easily cracked, and should not be used. A good alternative would be SFTP, which safely encrypts traffic. Additionally, SMB can provide significant information disclosure and even a remote shell if improperly configured or unpatched. The attack surface for SMB should be minimized and restricted to LANs.

Below is a Wireshark capture of a tool called psexec, connecting to an SMB share dropping an executable. This tool can be used by attackers to gain access to a session on the victim computer if the correct credentials are supplied.

If the attacker has network access to the computer and valid credentials, and port 445 is open on the target computer, this attack can be easily performed. The attacker drops an executable on the target machine, launches the executable as a temporary service, and pipes the screen keyboard output to the attacker, giving the attacker access to the target computer.

Another SMB shortcoming is transfer speed. Each SMB transfer is a limited number of bytes for request, depending on the version being used. These requests must be repeated until the end of the file transfer is reached. Each time the request reaches the data limit, a new request will be issued and each of these requests take away from transfer time. The SFTP behaves faster in this case as well, but also has its own shortcomings.

In short, the SMB protocol is antiquated, but the infrastructures built on top of this protocol will not change anytime soon. Although there are benefits to the protocol such as ease of use, there are still overarching problems. Hackers and penetration testers will continue to use SMB as an attack vector until the protocol evolves to be more secure, or is no longer needed for a Windows network to function.