به نام خدا

اسماعیل زارع

پروتکل SMB

SMBیا Server Message Block پروتکلی جهت به اشتراک‌گذاری فایل‌ها، چاپگرها و پورت‌های سریال است. از این پروتکل می‌توان بر روی پروتکل TCP/IP یا بر روی دیگر پروتکل‌های شبکه استفاده کرد. با استفاده از پروتکل SMB یک برنامه کاربردی (یا کاربر یک برنامه کاربردی) می‌تواند به فایل‌های و فولدر های موجود روی یک سرور و دیگر منابع آن از جمله چاپگر دسترسی داشته باشد. به عبارت دیگر یک برنامه کاربردی می‌تواند فایل‌هایی را از روی سرور بخواند، ایجاد کند و یا بروزرسانی کند. هم چنین می‌تواند با هر برنامه‌ی سرور که برای دریافت درخواست‌های کلاینت SMB راه اندازی شده است ارتباط برقرار کند. در حقیقت می‌توان گفت SMB یک پروتکل درخواست–پاسخ است که با استفاده از آن کلاینت درخواست SMB را به سمت سرور می‌فرستد و سرور نیز در جواب پاسخی از نوع SMB به کلاینت باز می‌گرداند.سیستم عامل ویندوز از پروتکل SMB پشتیبانی می‌کند NetBIOS) براساس این پروتکل کار می‌کند .(در سیستم عامل‌های مبتنی بر یونیکس مانند لینوکس و مک، برنامه Samba از این پروتکل جهت به اشتراک‌گذاری فایل‌ها بین سیستم عامل‌های مختلف (مثلا به اشتراک‌گذاری فایل بین یک سیستم لینوکسی و یک سیستم ویندوزی) بهره می‌برد .

پروتکل SMB یا Server Message Block یک پروتکل لایه ۷ می‌باشد که در سیستم عامل قرار دارد. پروتکل Server Message Blockمی تواند با لایه Session(ولایه های پایین تر) به راه های گوناگونی فعالیت کند :

- مستقیما روی پورت ٤٤٥ TCP
- از طریق API مربوط بهNetBIOS ، که در نتیجه می‌تواند روی چند پروتکل لایه Transport نیز فعالیت کند .
- روی پورتهای 137,138 UDP و TCP 137,139 NetBIOS over TCP/IP

روش های پیاده سازی SMB

۱- روش کلاینت_سرور

SMBاز طریق روش کلاینت_سرور، طوری که کلاینت درخواست‌های معینی ارسال می‌کند و سرور به آنها پاسخ می‌دهد، عمل می‌کند. یک قسمتی از پروتکل SMB صریحا به دسترسی به File System رسیدگی می‌کند (به طوری که کلاینت‌ها درخواست‌هایی را برای File Server ارسال می‌کنند)، اما قسمت‌های دیگر پروتکل SMB به IPC اختصاص دارند IPC Share .یا همان IPC$ یک Shareشبکه‌ای روی کامپیوترهای ویندوزی می‌باشد. از این Share مجازی به منظور سهولت ارتباط بین پردازش‌ها و کامپیوترها از روی پروتکل) SMB اغلب برای رد و بدل کردن اطلاعات بین کامپیوترهایی که احراز هویت شده‌اند) استفاده می‌شود .سازندگان و توسعه‌دهندگان نرم افزاری پروتکل SMB را برای استفاده شبکه محلی (Local Network)بهینه کرده‌اند، اما کاربران پروتکل SMBرا برای دسترسی به شبکه های مختلف درون اینترنت نیز به کار گرفته‌اند (Exploitهای مربوط به اشتراک فایل و پرینتر در محیط ویندوز معمولا روی این کاربرد متمرکز می‌شوند) سرورهایSMB ، Files Systemو دیگر منابع خود را در دسترس

کلاینت‌های شبکه قرار می‌دهند. کامپیوترهای کلاینت ممکن است نیاز به دسترسی بهFile System ها و پرینترهای به اشتراک گذاشته شده روی سرور داشته باشند، و در این کاربرد مقدماتی و اولیه، SMBبه عنوان مشهورترین و پُرکاربردترین شناخته شده است. به هر حال، جنبه سرورگونه SMB بدون بسته پروتکل‌های مبتنی بر دامین‌هایNT (که حداقل کار آنها، فراهم کردن احراز هویت تحت دامین‌های بر پایه NT می‌باشد) چندان کاربردی ندارد. تقریبا تمامی سرورهای SMB از احراز هویت دامین‌های NTبرای تائید سطح دسترسی کاربر به منابع استفاده می‌کنند .

Samba -۲

یک نرم افزار رایگان با هسته پروتکل SMB/CIFS است که اولین بار توسط Andrew Tridgellایجاد گردید. از نسخه ۳ و پس از آن، SAMBAسرویس‌های فایل و پرینت را برای کلاینت ویندوز فراهم کرده و می‌تواند با سرور دامین مبتنی بر Windows NT 4.0، به عنوان دامین کنترلر اصلی (PDC) یا به عنوان عضو دامین(Domain Member) ، ادغام شود. نسخه Samba4 می تواند به عنوان دامین کنترلراکتیو دایرکتوری و یا عضوی از دامین رویFunctional Levell های دامین و فارست ویندوز ۲۰۰۸ (Windows 2008 domain & forest Functional Level)عمل نماید .

ورژن‌های مختلف پروتکل SMB

اولین نسخه SMB با نام SMB شناخته نمی شود، در واقع با نام سیستم فایل رایج اینترنت (Common Internet File System) رایج (CIFS) است که اولین نسخه این پروتکل را نشان می دهد. همانطور که به شما گفته می شود که از زمان ایجاد ویندوز NT 4.0، کاملا جدید نیست .

پس از آن، و دقیق تر از ویندوز ۲۰۰۰، اولین نسخه پروتکل SMB وارد شده است. در اینجا خلاصه ای از نسخه های پروتکل SMBذکر شده است :

(1984) SMB 1.0 :ایجاد شده توسط آی بی ام برای به اشتراک گذاری فایل در .DOS قفل اپورتونیستی (OpLock) را به عنوان یک مکانیزم ذخیره سازی برای مشتری طراحی کرده تا ترافیک شبکه را کاهش دهد.

(1996) CIFS : زبان SMB توسعه یافته مایکروسافت که در ویندوز ۹۵ عرضه شده است. پشتیبانی از اندازه فایل های بزرگتر، انتقال مستقیم بر روی TCP / IP و لینک های نمادین و لینک های سخت افزوده شده است.

(2006) SMB 2.0 :با ویندوز ویستا و ویندوز سرور ۲۰۰۸ منتشر شده است. برای بهبود عملکرد، مقیاس پذیری و انعطاف پذیری افزایش یافته و پشتیبانی از شتاب WAN افزوده شده است.

SMB 2.1 (2010) :با ویندوز سرور ۲۰۰۸ R2 و ویندوز ۷ معرفی شده است. مدل لیزینگ مشتری oplock جایگزین OpLock برای افزایش ذخیره و بهبود عملکرد است. به روز رسانی های دیگر شامل پشتیبانی از حداکثر انتقال حداکثر (MTU) و بهبود بهره وری انرژی است که مشتریان را با فایل های باز از یک سرور SMB به حالت sleep فعال می کند.

SMB 3.0 (2012) :در ویندوز ۸ و ویندوز سرور ۲۰۱۲ عرضه شده است. برای بهبود در دسترس بودن، عملکرد، تهیه نسخه پشتیبان، امنیت و مدیریت، چندین نسخه قابل ارتقا وجود دارد. قابل توجه ویژگی های جدید شاملSMB Multichannel ، SMBمستقیم، شکستن شفاف دسترسی مشتری پشتیبانی از VSS از راه دور، رمزگذاری SMB و بیشتر.

SMB 3.02 (2014) :در ویندوز ۸٫۱ و ویندوز سرور ۲۰۱۲ R2 معرفی شده است. شامل به روز رسانی عملکرد و توانایی به طور کامل غیر فعال کردن پشتیبانیSMB 1.0 / CIFS ، از جمله: حذف باینری مربوط.

SMB 3.1.1 (2015): با ویندوز ۱۰ و ویندوز سرور ۲۰۱۶ منتشر شده است. پشتیبانی از رمزنگاری پیشرفته، یکپارچگی قبل از شناسایی برای جلوگیری از حملات در یک سو مردانه و شمشیر گویش خوشه ای، از سوی دیگر به روز رسانی ها اضافه شده است. در سال ۲۰۱۷ حملات WannaCry و Petya ransomware یک آسیب پذیری در SMB 1.0 را برای بارگیری نرم افزارهای مخرب بر روی مشتریان آسیب پذیر و گسترش آن در بین شبکه ها مورد استفاده قرار دادند. مایکروسافت پس از آن یک پچ را منتشر کرد، اما متخصصان توصیه کرده اند که کاربران و مدیران گام دیگری برای غیر فعال کردن SMB 1.0 / CIFS در تمام سیستم ها داشته باشند.

گزارش آسیب پذیری CVE-2020-1301 در SMBv1

آسیب پذیری CVE-2020-1301 از نوع اجرای کد از راه دور می باشد که با شدت خطر CVSS 7.5شناخته شده است. مهاجم احراز هویت شده، برای بهره برداری موفق از این آسیب پذیری تنها نیاز به ساخت و ارسال یک پکت خاص به سمت سرور مورد هدف دارد. این آسیب پذیری از عدم برخورد صحیح SMBv1 با درخواست های ورودی از سمت کاربر نشات می گیرد.

نسخه های آسیب پذیر:

- Windows 10 Version 1809 for x64-based Systems Windows 10 for 32-bit Systems
- Windows 10 Version 1903 for 32-bit Systems Windows 10 for x64-based Systems
- Windows 10 Version 1903 for ARM64-based Systems Windows 10 Version 1607 for 32-bit Systems
- Windows 10 Version 1903 for x64-based Systems Windows 10 Version 1607 for x64-based Systems

- Windows 10 Version 1909 for 32-bit Systems Windows 10 Version 1709 for 32-bit Systems
- Windows 10 Version 1909 for ARM64-based Systems Windows 10 Version 1709 for ARM64-based Systems
- Windows 10 Version 1909 for x64-based Systems Windows 10 Version 1709 for x64-based Systems
- Windows 10 Version 2004 for 32-bit Systems Windows 10 Version 1803 for 32-bit Systems
- Windows 10 Version 2004 for ARM64-based Systems Windows 10 Version 1803 for ARM64-based Systems
- Windows 10 Version 2004 for x64-based Systems Windows 10 Version 1803 for x64-based Systems
- Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for 32-bit Systems
- Windows RT 8.1 Windows 7 for 32-bit Systems Service Pack 1
- Windows Server 2008 for 32-bit Systems Service Pack 2 Windows 7 for x64-based Systems Service Pack 1
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows 8.1 for 32-bit systems
- Windows Server 2008 for Itanium-Based Systems Service Pack 2 Windows 8.1 for x64-based systems
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
- Windows Server 2012 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2012 R2 Windows Server 2012 (Server Core installation)
- Windows Server 2016 Windows Server 2012 R2 (Server Core installation)
- Windows Server 2019 Windows Server 2016 (Server Core installation)
- Windows Server, version 1803 (Server Core Installation) Windows Server 2019 (Server Core installation)
- Windows Server, version 1909 (Server Core installation) Windows Server, version 1903 (Server Core installation)
- (Windows Server, version 2004 (Server Core installation)

بروز رسانی جدیدی برای مرتفع سازی این آسیب پذیری انتشار یافته است، شما می توانید با مراجعه به لینک زیر اطلاعات بیشتری متناسب با نسخه مورد استفاده خود دریافت نمایید.

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1301

همچنین پیشنهاد می شود تا SMbv1 را غیر فعال نمایید:

کاربران Windows 8.1 یا Windows Server 2012 R2 می توانند طبق مراحل زیر اقدام به غیر فعال سازی نمایند.

۱. Open Control Panel, click Programs, and then click Turn Windows features on or off.

۲. In the Windows Features window, clear the SMB1.0/CIFS File Sharing Support checkbox, and then click OK to close the window.

۳. Restart the system.

کاربران سیستم عامل های سرور نیز می توانند از مراحل زیر اقدام نمایند.

۱. Open Server Manager and then click the Manage menu and select Remove Roles and Features.

۲. In the Features window, clear the SMB1.0/CIFS File Sharing Support check box, and then click OK to close the window.

۳. Restart the system.

جدول زیر نشان دهنده نسخه ای از SMB است که در نهایت می‌تواند استفاده شود (بسته به اینکه چه نسخه ویندوز به عنوان SMB client و SMB server اجرا می شود:)

OS	Windows 8.1 WS 2012 R2	Windows 8 WS 2012	Windows 7 WS 2008 R2	Windows Vista WS 2008	Versions précédentes
Windows 8.1 WS 2012 R2	SMB 3.02	SMB 3.0	SMB 2.1	SMB 2.0	SMB 1.0
Windows 8 WS 2012	SMB 3.0	SMB 3.0	SMB 2.1	SMB 2.0	SMB 1.0
Windows 7 WS 2008 R2	SMB 2.1	SMB 2.1	SMB 2.1	SMB 2.0	SMB 1.0
Windows Vista WS 2008	SMB 2.0	SMB 2.0	SMB 2.0	SMB 2.0	SMB 1.0
Versions précédentes	SMB 1.0	SMB 1.0	SMB 1.0	SMB 1.0	SMB 1.0

ویژگی های پروتکلSMB

با بالا رفتن نسخه های SMB ، سطح عملکرد آن نیز افزایش می یابد. در ادامه چند ویژگی مهم SMB آورده شده است:

۱. پروتکل SMB یک مکانیزم فرآیند ارتباط متقابل تأیید شده برای به اشتراک گذاشتن فایل ها یا منابع دیگر مثل پوشه ها یا پرینتر ها در سرور فراهم می کند.

۲. پروتکل SMB به مشتریان امکان ویرایش فایل ها، حذف آنها، اشتراک گذاری فایل ها، مرور شبکه، خدمات چاپ و غیره را از طریق شبکه فراهم می کند.

۳. نسخه ۲ پروتکل SMB میزان استفاده از دستورات و زیرمجموعه های آن برای انتقال فایل به سراسر اینترنت را کم کرده .

٤. SMB2ازسیلینک یا سافت لینک که یک نوع لینک است که در آن به لینک یا دایرکتوری دیگر ارجاع داده شده است هم پشتیبانی میکند.

انواع بسته های اطلاعاتی در Server Message Block

بسته‌های کنترل جلسه (Session) که وظیفه ایجاد یا قطع ارتباطات مربوط به اشتراک گذاری منابع را برعهده دارند.

- بسته‌های مجوز دسترسی که به کلاینت اجازه دسترسی و تغییر دادن اطلاعات را می‌دهند.
- بسته‌هایی که پیغام‌ها را گروه بندی کرده و یک بار انتقال می‌دهند تا پهنای باند شبکه افزایش و زمان تاخیر کاهش یابد. که اصطلاحا به آن Packet Batching گفته می‌شود.

امنیت در پروتکلSMB

با توجه به نوع کاربرد و فعالیت پروتکل SMB قطعا یکی از پروتکل‌هایی است که در حملات خرابکارانه مورد هدف هکرها قرار می‌گیرد. زیرا هکرها با نفوذ به پروتکل SMB و دستکاری قوانین وضع شده در آن می‌توانند به اطلاعات و منابع مشترک شبکه دسترسی پیدا کرده و از آنها سوء استفاده کنند.

در پروتکل SMB دو نوع امنیت مطرح است، امنیت کاربر و امنیت اشتراک گذاری منابع:

امنیت کاربر: هر کاربر برای دسترسی به اطلاعات و منابع مشترک شبکه نیاز به یک نام کاربری و رمز عبور منحصر به فرد دارد.

امنیت اشتراک گذاری منابع: در این نوع امنیت، کاربری که با نام کاربری و رمز عبور معتبر احراز هویت شده است و به منابع شبکه دسترسی پیدا کرده است سطح بندی می‌شود و به طور کامل به تمام منابع دسترسی نخواهد داشت.

به عنوان مثال یک شرکت را در نظر بگیرید که دارای یک سرور برای اشتراک گذاری منابع اطلاعاتی است. تمام کارمندان شرکت با داشتن یک نام کاربری و رمز عبور مخصوص خودشان احراز هویت می‌شوند و به سرور لاگین می‌کنند. اما هر کاربر براساس نیاز به قسمت‌های مختلف دسترسی دارد، به طور مثال کارمند بخش اداری به پرونده‌های پرسنلی دسترسی دارد ولی دسترسی او به فاکتورهای فروش کالا بسته است.

هر دو موردی که در مثال بالا بیان شد دو روش مهم برای حفظ امنیت SMB هستند که پیاده سازی درست این روش‌ها تاثیر بالایی در حفظ امنیت شبکه و منابع آن دارد.

حملات مبتنی بر پروتکلSMB

در حملات مبتنی بر پروتکلSMB ، فرد مهاجم خود را وارد مسیر یک تبادل اطلاعات میکند، به این صورت که فرد سرور هدف که قصد تأیید اعتبار آن را دارد را انتخاب می کند و سپس منتظر می ماند تا شخصی در شبکه سیستم او را تأیید اعتبار کند.

حملات SMB از مهم ترین حملات شناخته شده برای اجرای کد در سیستم های ویندوز است و از آنجا که این یک حمله کد از راه دور است، مهاجمان می توانند در هر مکانی باشند. آنها فقط باید آسیب پذیری های یک سیستم را شناسایی کنند، از این امر سوء استفاده کنند، دستوراتی را روی سیستم اجرا کنند، بدافزارها را در محل مورد نظر قرار دهند و در مرحله بعد حمله انجام میشود.

از مزیت های حملات مبتنی بر پروتکل SMB این است که مهاجمان میتوانند دسترسی خود را در سیستم یه صورت جانبی گسترش دهند .

سیستم های ویندوز بدون پچ می توانند هنگام اتصال به یک سیستمی که آلوده شده است، آلوده شوند و این حمله به نسبت نتیجه بالایی که میگیرد نیاز به تلاش کمتری دارد ، به همین دلیل حملات مبتنی بر پروتکل SMB بسیار رایج است.

معروف ترین حمله ای که روی پروتکل SMB انجام میشود حمله WannaCry است .این حمله از آسیب پذیری زیاد پروتکل SMB با سوء استفاده از EternalBlue صورت گرفت و در سراسر جهان برای یک سال و نیم ادامه داشت.

نمونه دیگر سوء استفاده از EternalBlue ، حمله Emotet است که بانک ها را مورد هدف قرار می دهد. از سوء استفاده های دیگر از ضعف پروتکل SMB میتوان به EternalRomance و Bad Rabbit و EternalEnergy اشاره کرد .

محققان امنیتی یک آسیب پذیری حساس جدید را تحت عنوان "SMBleed" در پروتکل SMB کشف کرده اند که می تواند به مهاجمان اجازه دهد به حافظه داخلی از راه دور نفوذ کنند و هنگامی که با یک SMBGhost ترکیب شود ، به مهاجمان اجازه می دهد تا کنترل RCE روی سرور یا SMB client را بدست آورند .SMBGhost تهدیدی است که در سال ۲۰۲۰ گزارش داده شده و روی ویندوز ۱۰ در صورتی که پچ نداشته باشد اثر میگذارد .

رفع آسیب پذیری پروتکلSMB

یکی از ساده ترین راه ها برای رفع این مشکل این است که پچ هایی که ویندوز برای ایرادات خود منتشر کرده را روی سیستم خود نصب کنید. البته این حمله ها بیشتر روی ویندوز پایین تر از ۱۰ صورت می گیرد، پس در صورتی که سیستم شما ویندوز ۱۰ است، این پچ ها روی سیستم شما به صورت پیش فرض قرار دارد.

یکی از راه های دیگر این است که شما ورودی و خروجی شبکه خود را به صورت انتخابی قرار دهید. مثلا فقط اجازه تبادل فایل های SMB و backup ها و ترافیک های کنترل کننده های دامنه را بدهید و بقیه ترافیک ها محدود شود .

البته درصورتی که ویندوز شما پچ ندارد، بهترین راه امن بودن در مقابل حملات مربوط بهSMB ، استفاده نکردن از این پروتکل می‌باشد. در واقع از سال 2018این پروتکل به صورت پیش فرض در ویندوز نصب نشده است. از آن پس برای به اشتراک گذاری فایل‌ها از یک سرور فایل اختصاصی یا یک راهکار مبتنی بر Cloudبایداستفاده کرد؛ برای استفاده از پرینترهای شبکه ای هم از پروتکل های دیگر استفاده می شود .

در صورتی که نمیخواهید یا نمیتوانید پروتکل SMB خود را خاموش کنید، حداقل SMB1 را غیر فعال کنید