

به نام خدا

اسماعیل زارع

پروتکل SMB

SMB یا 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 فولدرهای 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 Block می‌تواند با لایه Session (ولایه‌های پایین تر) به راه‌های گوناگونی فعالیت کند :

- مستقیماً روی پورت ۴۴۵ TCP
- از طریق API مربوط به NetBIOS ، که در نتیجه می‌تواند روی چند پروتکل لایه Transport نیز فعالیت کند .
- روی پورتهای 137,138 UDP و 137,139 NetBIOS over TCP/IP

روش‌های پیاده‌سازی SMB

۱- روش کلاینت_سرور

SMB از طریق روش کلاینت_سرور، طوری که کلاینت درخواست‌های معینی ارسال می‌کند و سرور به آنها پاسخ می‌دهد، عمل می‌کند. یک قسمتی از پروتکل SMB صریحاً 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 Share شبکه‌ای 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 SMB را برای دسترسی به شبکه‌های مختلف درون اینترنت نیز به کار گرفته‌اند (Exploit های مربوط به اشتراک فایل و پرینتر در محیط ویندوز معمولاً روی این کاربرد متمرکز می‌شوند) سرورهای SMB ، Files System و دیگر منابع خود را در دسترس

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

۲- Samba

یک نرم افزار رایگان با هسته پروتکل SMB/CIFS است که اولین بار توسط Andrew Tridgell ایجاد گردید. از نسخه ۳ و پس از آن، SAMBA سرویس‌های 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 Samba 4 می‌تواند به عنوان دامین کنترلر اکتیو دایرکتوری و یا عضوی از دامین روی Functional Level 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 نمی‌شود، در واقع با نام سیستم فایل رایج اینترنت (Common Internet File System) رایج (CIFS) است که اولین نسخه این پروتکل را نشان می‌دهد. همانطور که به شما گفته می‌شود که از زمان ایجاد ویندوز NT 4.0، کاملاً جدید نیست.

پس از آن، و دقیق‌تر از ویندوز ۲۰۰۰، اولین نسخه پروتکل SMB وارد شده است. در اینجا خلاصه‌ای از نسخه‌های پروتکل SMB ذکر شده است:

- CIFS زبان SMB توسعه یافته مایکروسافت است که در ویندوز ۹۵ عرضه شده است. پشتیبانی از اندازه فایل‌های بزرگتر، انتقال مستقیم بر روی TCP/IP و لینک‌های نمادین و لینک‌های سخت افزوده شده است.
- SMB 1.0: اولین نسخه با نام SMB با ویندوز ۲۰۰۰ وارد شد و توسط ویندوز ایکس پی، ویندوز سرور ۲۰۰۳ و ویندوز سرور ۲۰۰۳ R2 استفاده شد.
- SMB 2.0: نسخه مورد استفاده در ویندوز ویستا (SP1) و بالاتر (و معادل سرور آن یعنی ویندوز سرور ۲۰۰۸)
- SMB 2.1: نسخه مورد استفاده در ویندوز ۷ و ویندوز سرور ۲۰۰۸ R2.
- SMB 3.0: تولد پروتکل SMB v3 با راه اندازی ویندوز ۸ و ویندوز سرور ۲۰۱۲.
- SMB 3.02: که در ویندوز ۸.۱ و ویندوز سرور ۲۰۱۲ R2 معرفی شده است.
- SMB 3.1.1: با ویندوز ۱۰ و ویندوز سرور ۲۰۱۶ منتشر شده است.

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 می‌شود):

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 پروتکل SMB

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

۱. پروتکل SMB یک مکانیزم فرآیند ارتباط متقابل تأیید شده برای به اشتراک گذاشتن فایل‌ها یا منابع دیگر مثل پوشه‌ها یا پرینترها در سرور فراهم می‌کند.
۲. پروتکل SMB به مشتریان امکان ویرایش فایل‌ها، حذف آنها، اشتراک گذاری فایل‌ها، مرور شبکه، خدمات چاپ و غیره را از طریق شبکه فراهم می‌کند.
۳. نسخه ۲ پروتکل SMB میزان استفاده از دستورات و زیرمجموعه‌های آن برای انتقال فایل به سراسر اینترنت را کم کرده.
۴. SMB2 از سیلینک 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 اصطلاحاً به آن Packet Batching گفته می‌شود.

امنیت در پروتکل SMB

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 پروتکل SMB

در حملات مبتنی بر پروتکل SMB، 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 می‌کند و سپس منتظر می‌ماند تا شخصی در شبکه سیستم او را تأیید اعتبار کند.

حملات SMB از مهم‌ترین حملات شناخته شده برای اجرای کد در سیستم‌های ویندوز است و از آنجا که این یک حمله کد از راه دور است، مهاجمان می‌توانند در هر مکانی باشند. آنها فقط باید آسیب‌پذیری‌های 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 مزیت‌های حملات مبتنی بر پروتکل SMB این است که مهاجمان میتوانند دسترسی خود را در سیستم به صورت جانی گسترش دهند.

سیستم‌های ویندوز بدون پچ می‌توانند 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 پروتکل SMB

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. مثلاً 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 در صورتی که ویندوز شما پچ ندارد، بهترین راه امن بودن در مقابل حملات مربوط به SMB ، استفاده نکردن از این پروتکل می باشد. در واقع از سال ۲۰۱۸ این پروتکل به صورت پیش فرض در ویندوز نصب نشده است. از آن پس برای به اشتراک گذاری فایل ها از یک سرور فایل اختصاصی یا یک راهکار مبتنی بر Cloud باید استفاده 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