راهنمای مشکل امنیتی موجود بر روی MSSQL

راهنمای مشکل امنیتی موجود بر روی MSSQL

تاریخ تنظیم : مرداد ۱۳۹۸

گروه شرکت‌های شاتل

Microsoft SQL Serverیک بانک اطلاعاتی از نوع دیتابیس های رابطه ای یا Relational Database می باشد که توسط کمپانی Microsoft ارایه شده و وظیفه اصلی آن ذخیره و بازیابی اطلاعات بر اساس درخواست نرم افزارهای دیگر میباشد. مهاجم ها از تکنیک های جدید مربوط به بازتاب MS SQL استفاده میکنند و می توانند پروتکل مربوط به بازتاب MSSQL را تحت تاثیر قرار داده و حملات DDOS را راه اندازی کنند .

برای اجرای حمله، فرد حمله‌کننده یک درخواست تحلیل سرور MSSQL را برای سرویس‌دهنده MSSQL ارسال می نماید ولی به‌جای قرار دادن آدرس IP خود در فیلد آدرس IP فرستنده، آدرس IP فرد قربانی را قرار می‌دهد. درنتیجه پاسخ تولیدی توسط MSSQL برای فرد قربانی ارسال خواهد شد. به دلیل اینکه تعداد بایت موجود در پیامی که سرور در پاسخ باز می‌گرداند نسبت به تعداد بایت موجود در پرسش ارسال شده از سوی کلاینت قابل توجه است، حمله‌کننده می‌تواند به ضریب تقویت بالایی دست پیدا کند. بدین صورت با به‌کارگیری یک شبکه باتنت می‌توان ترافیک بسیار زیادی به سوی فرد قربانی هدایت نمود. درنتیجه یک سرویس‌دهنده MSSQL که پیکربندی صحیحی ندارد می‌تواند به‌طور ناخواسته در حمله DDoS مورد سوءاستفاده قرار گیرد.

MSSQL دسترسی از راه دور را از طریق یک رابط Open Database Connectivity (ODBC) ایجاد می کند که به صورت پیش فرض بر روی پورت ۱۴۳۳ کار می کند. پس از برقراری ارتباط با این رابط از کاربران شناسه و رمز عبور دریافت می شود. در MSSQL اکانتی به نام "sa" به صورت پیش فرض وجود دارد که دسترسی مدیریت پایگاه داده از طریق این اکانت فعال است. هکرها می توانند از این اطلاعات استفاده کنند و با اجرای یک حمله Brute Force و با استفاده از پسوردهای معمول اطلاعات ورودی را پیدا کرده و بر روی پایگاه داده MSSQL لاگین کنند.

پس از لاگین بر روی پایگاه داده، علاوه بر دسترسی به اطلاعات موجود در آن با ایجاد مقداری تغییرات در تنظیمات پایگاه داده (فعال کردن قابلیت xp_cmdshell)، هکر می تواند به Command-line سرور نیز دسترسی پیدا کرده و از این طریق فایروال و آنتی ویروس سرور را غیر فعال کند. به محض غیر فعال شدن آنتی ویروس، هکرها می توانند با استفاده از این فرصت انواع بدافزارها مانند Key logger ها، Malwareها، ابزارهای دسترسی از راه دور و استخراج کننده های ارزهای مجازی و غیره را بر روی سیستم مورد حمله اجرا کنند و مشکلات متعددی را برای سرور و شبکه آن ایجاد کنند.

در صورتی که شما در حال اجرا و استفاده از MSSQL و یا حتی MySQL هستید, لازم است برای حفظ اطلاعات خود پایگاه داده خود را ایمن و خصوصی نگه دارید .

جهت بالا بردن امنیت MSSQL میتوانید موارد زیر را بررسی بفرمایید :

لزوم استفاده از MS-SQL را بررسی کنید

بررسی کنید که آیا به‌راستی نیاز است که از MS-SQL در شبکه خود استفاده کنید یا خیر؟ در صورت عدم نیاز به این سرویس حتماً آن را در شبکه خود غیرفعال کنید.

IP Blacklistsو IP Whitelists را پیاده سازی کنید

برای ایجاد ارتباط با سرورهای خود، سعی کنید لیست مشخصی از IP های مجاز و غیرمجاز تهیه‌کرده و آن را بر روی Firewall های نرم‌افزاری و یا سخت‌افزاری خود محدود کنید.

برای اولین راه، حتماً ارتباط با سرورهای خود را از طریق سرورهای خارج از ایران ببندید.

سرورهای پایگاه داده معمولا تنها با یک سرور دیگر (یا چندین سرور مشخص) متصل می شوند؛ در اینصورت لازم است دسترسی به سرور بر روی پورت های پایگاه داده از هر جای دیگری مسدود شود. با اجازه دادن به انتقال ترافیک SQL از طریق ادرس های IP مشخص شده میتوان اطمینان حاصل کرد که یک مخرب یا یک متقاضی آلوده به سرورمان ضربه نمیزند . در برخی موارد، مشتریان باید مستقیما به خود کارگزار پایگاه‌داده متصل شوند که در اینصورت می توان از Remote VPN های ایمن مانند IPsec استفاده کرد.

سرور پایگاه داده را جدا سازی کنید

لازم است سرور های پایگاه داده از سایر برنامه ها و سرویس ها جدا شوند . بر روی سرور پایگاه داده به جز برنامه هایی که سرور پایگاه داده به آن نیاز دارد برنامه های دیگر را نصب نکنید. این امر نه تنها باعث امنیت بیشتر، بلکه باعث جلوگیری از Fragmentation می شود.

ویژگی های اضافی و غیر قابل استفاده در کار شما را حذف کنید

MSSQL و همچنین MySQL دارای ویژگی های متنوع زیادی هستند و در خیلی موارد نیاز به همه این ویژگی ها نیست. برای بالاتر بردن امنیت و کاهش احتمال ورود ناخواسته به سیستم بهتر است ویژگی هایی که نیاز ندارید را حذف کنید .

فرآیندهای DB را محدود کنید

فرآیند های دسترسی پایگاه داده (از جمله فایل های سیستمی, توانایی اجرای برنامه ها و غیره) توسط کاربری که تحت آن سرویس پایگاه داده را اجرا میکنید به بقیه سرور اختصاص داده می‌شود. همانند اکثر برنامه های لینوکس MySQL به طور معمول تحت یک حساب کاربری اختصاصی با کمترین دسترسی به بقیه سرور اجرا می‌شود. شما می توانید با یک دستور ساده ps اطمینان حاصل کنید که MySQL به صورتی پیکربندی نشده است که به صورت root اجرا شود. در برخی مانند عیب یابی در زمان از کار افتادن MySQL به عنوان root اجرا میشود که پس از رفع بحران باید مجدد به صورت قبل پیکربندی شود.

اما در نصب ویندوز، MSSQL اغلب به عنوان سیستم محلی یا یک حساب کاربری مدیر اجرا می شود، که اجازه می دهد فرایندهای پایگاه داده، از جمله روش های ذخیره شده و رابط های فرماندهی مانند xp_cmdshell، دسترسی کامل داشته باشند . در حالت ایده آل، MSSQL باید به عنوان یک حساب محلی اختصاصی و غیر مجاز با حداقل امتیازات اجرا شود. Wizard های نصب جدیدتر MS می توانند این مرحله را برای شما انجام دهند. بنابراین اگر شما یک سرور جدید نصب می کنید، مطمئن شوید که این گزینه را پیکربندی کنید. دیگر خدمات SQL مانند SQL Agent نیز باید به عنوان اکانت های داخلی محدود ، با مجوز هایی که تنها مورد نیاز است استفاده شوند ، به عنوان مثال دایرکتوری پشتیبان.
عدم انجام این مرحله می تواند باعث شود که یک سرور پایگاه داده به خطر افتاده را مجاز به برقراری ازتباط با سایر دستگاه ها بوده و احتمال نفوذ به شبکه را بالا ببرد.

مجوز به کاربران را به میزان نیاز آنها اعطا کنید

کاربران پایگاه داده، لازم است تنها به اندازه نیاز خود برای انجام وظایف دسترسی داشته باشند.
در صورتی که امکان دارد، «ALL» را در MySQL و عضویت نقش Sysadmin در MSSQL غیرفعال کنید. و به منظور حفاظت از موارد حساس سعی کنید از دسترسی های View به جای دسترسی مستقیم به جداول استفاده کنید.

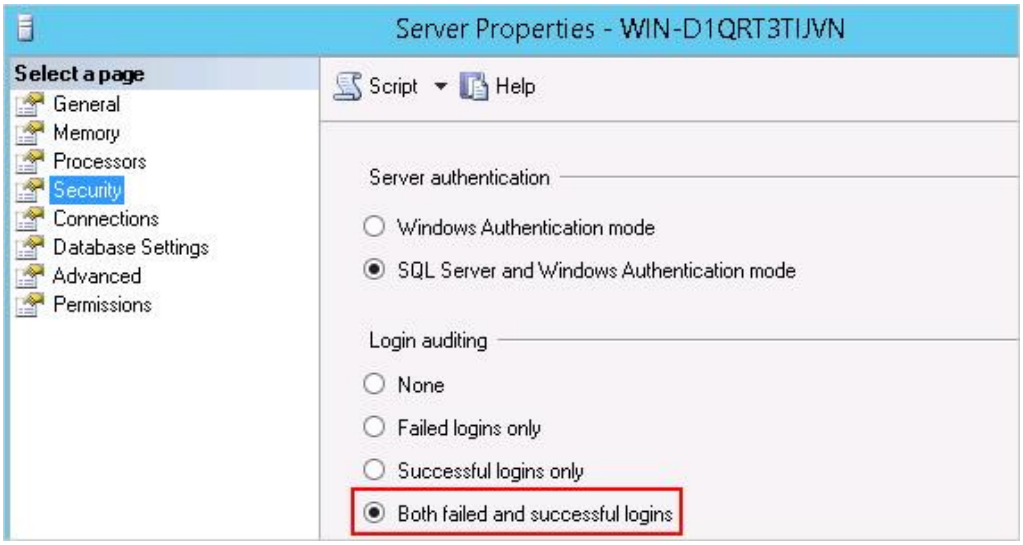
یک رمز عبور قوی استفاده کنید

در MSSQL، اکانت SA در زمان انتخاب mixed-mode authentication استفاده می شود. اگر mixed-mode authentication را فعال کردید، مطمئن شوید که برای اکانت sa یک رمز عبور پیچیده انتخاب می کنید تا از brute forced جلوگیری شود.
به طور مشابه،کاربر root برای MySQL نیز باید یک رمز عبور پیچیده داشته باشد. اگر کسی سرورهای پایگاه داده را اسکن کند، اولین کاری که انجام می دهد این است که سعی کند به عنوان حساب کاربری پیش فرض به سیستم وارد شود؛ بنابراین عدم تعیین رمز عبور پیچیده می تواند منجر به سازش کامل سیستم شده و کل سرور در معرض خطر قرار میگیرد .

نظارت کلی و منظم بر ورود کابران داشته باشید

لازم است به صورت خودکار اطلاع رسانی های مورد نیاز به کاربران انجام پذیرد . این کار باعث میشود که بتوانید کابرانی که در خطر افتاده اند را پیدا کرده و آنها را غیر فعال کنید و یا پسورد ها را تغییر دهید. همچنین ورود های موفق و ناموفق را لاگ کنید. در این صورت می توانید از وقوع حملات brute forced مطلع شوید.
برای این کار

۱- SQL Server Management Studio را باز کنید و بر روی SQL Server که می خواهید در آن تغییرات انجام دهید کلیک راست کرده و Properties را انتخاب کنید.
۲- در قسمت چپ صفحه Server Properties می توانید Select a Page را ببینید؛ در این قسمت بر روی Security کلیک کنید. در صفحه جدید و در بخش Login auditing گزینه Both failed and successful logins را انتخاب کنید و OK کنید.



شکل 1

۳- SQL Server را Reboot کنید.

از دادن دسترسی root یا SA به نرم افزار هایی که در حال ارتباط با SQL هستند خودداری کنید و همانطور که در بالا ذکر شد، برای هر کاربر، با توجه به نیاز ایشان، دسترسی های مورد نیاز بر روی سرور و دیتابیس مورد نظر ساخته شود و هنگام اعطای دسترسی از انتخاب مواردی که از آن اطلاع ندارید خودداری کنید.

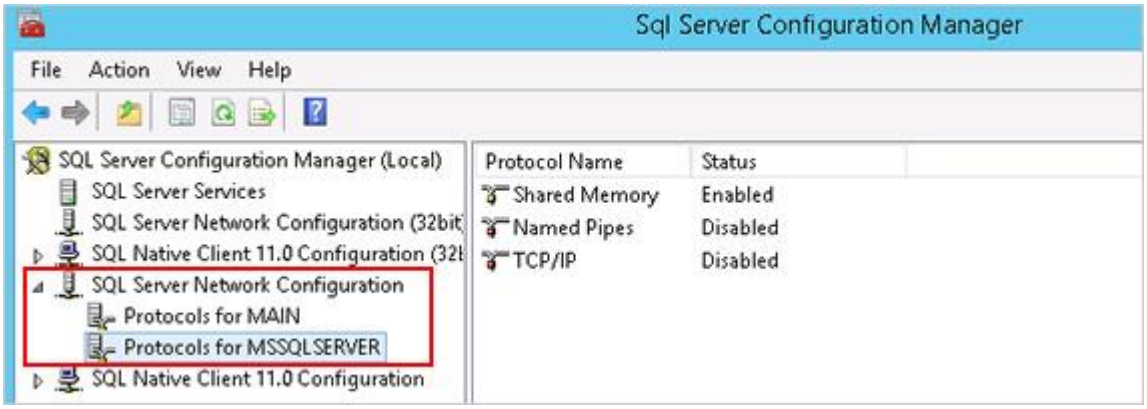
Backup هایتان را امن کنید

بک آپ های شما دارای داده های مشابه با پایگاه داده های اصلی شما هستند و نیاز به مراقبت بسیار زیادی دارند. منظور از مراقب بیشتر شامل مواردی همچون قفل کردن دایرکتوری های پشتیبان، محدود کردن دسترسی به سرور یا محل ذخیره سازی داده ها، امنیت فیزیکی رسانه های قابل جابجایی، محدودیت دسترسی به شبکه برای پشتیبان گیری و بررسی افرادی که دسترسی به بک آپ دارند و ... است.

پورت TCP پیش فرض پایگاه داده را تغییر دهید.

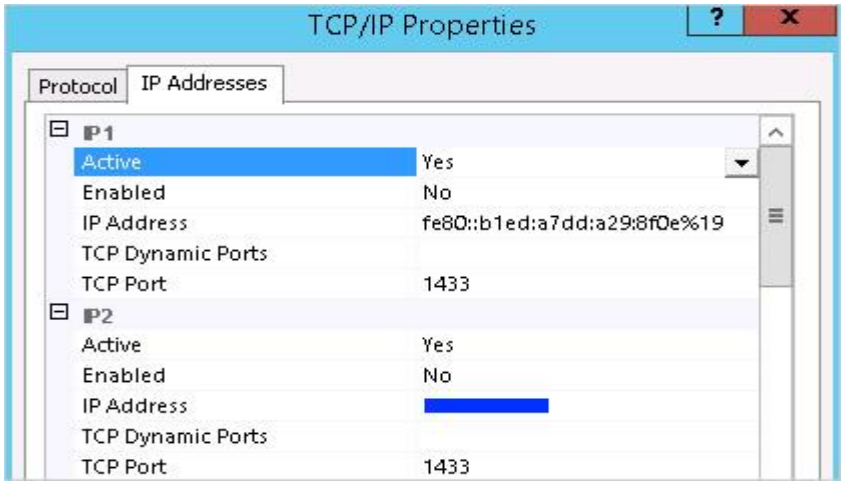
(در صورتی که امکان تغییر پورت وجود نداشته باشد از روش هایی مانند Port Forwarding و یا محدودیت سطح دسترسی روی فایروال میتوان استفاده کرد.)

۱- در SQL Server Configuration Manager منوی SQL Server Network Configuration را باز کنید. از منوی باز شده گزینه Protocols for the MSSQL SERVER را انتخاب کنید.



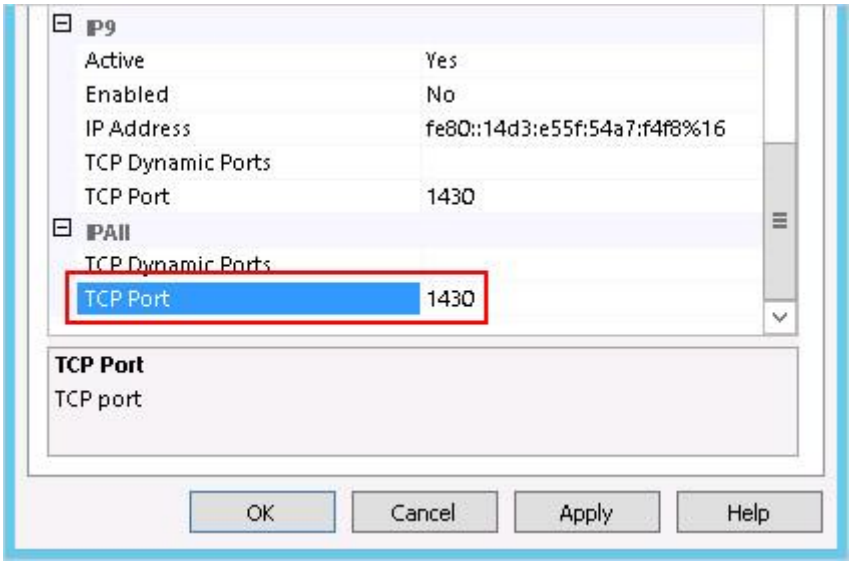
شکل 2

۲- گزینه TCP/IP را باز کنید و سپس بر روی تب IP Addresses کلیک کنید. در این قسمت لیستی شامل گزینه IP1 در ابتدا و IPAll در انتها مشاهده می کنید.



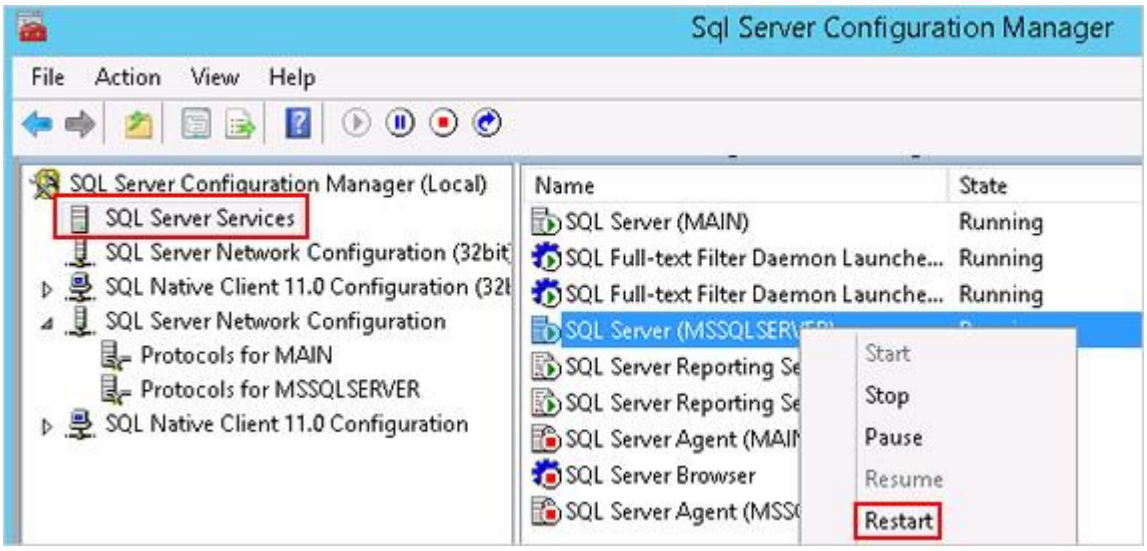
شکل 3

۳- شما می توانید در این صفحه برای هر IP پورت جداگانه در نظر بگیرید. یا در قسمت IPAll پورت را برای همه IP ها تغییر دهید. در قسمت TCP Dynamic Ports نیاز به وارد کردن هیچ مقداری نیست (اگر مقدار صفر از قبل وارد شده است آن را حذف کنید). پس از انجام تغییرات Apply را بزنید.



شکل 4

۴- در SQL Server Configuration Manager بر روی قسمت SQL Server Services کلیک کنید. در این صفحه شما باید SQL Server ی که قبلا انتخاب کرده و تغییرات را بر روی آن انجام داده بودید انتخاب کرده، پس از راست کلیک گزینه Restart را انتخاب کنید.



شکل 5

- پس از تغییر پورت لازم است در اپلیکیشن هایی که از این پایگاه داده استفاده می کنند نیز پورت را تغییر دهید.

اطلاعات با ارزش و حساس را رمزگذاری کنید.

SQL سرور به شما امکان رمزگذاری اطلاعات را به روش های کلید متقارن، کلید نامتقارن، استفاده از Certificate و استفاده از روش Transparent Data Encryption (TDE) می دهد که در روش آخر اطلاعات در سطح پایگاه داده و قبل از نوشتن آنها بر روی دیسک رمزگذاری می شود. TDE کل پایگاه داده را رمزگذاری می کند و زمانی که نیاز به دیدن اطلاعات باشد آنها را رمزگشایی می کند.

گزینه Xp_cmdshell را غیر فعال کنید

xp-cmdshell به طور گسترده‌ای جهت دریافت اطلاعاتی از سیستم عامل میزبان بانک اطلاعاتی(خواندن یا نوشتن)،توسط مهاجمین مورد استفاده قرار میگیرد.

رویه xp-cmdshell به کاربران اعتبارسنجی شده SQL اجازه می‌دهد تا دستورات سیستم عامل را از طریق آن اجرا نمایند ونتیجه را در SQL Client باز گردانند.

بااجرای فرمان زیر میتوان مشخص نمود که رویه xp-cmdshell فعال است یا خیر.

```
EXECUTE sp_configure 'show advanced options',1;
RECONFIGURE WITH OVERRIDE;
EXECUTE sp_configure 'xp_cmdshell';
```

شکل 6

اگر مقدار بازگشتی برای خروجی run_value صفر باشد،این رویه غیر فعال است.

با اجرای فرمان زیر،میتوان مقدار این امکان را غیرفعال ساخت:

```
EXECUTE sp_configure 'show advanced options', 1;
RECONFIGURE;
EXECUTE sp_configure 'Xp_cmdshell', 0;
RECONFIGURE;
EXECUTE sp_configure 'show advanced options', 0;
RECONFIGURE;
```

شکل 7