پروتکل مدیریتی شبکه (SNMP(Simple Network Management Protocol

علاوه بر سطوح کنترل کاربر، سطح مدیریت، یکی از سطوح معماری شبکه است که شامل پروتکل‌های مختلفی می‌باشد و از استاندارد SNMP می‌توان به عنوان یک پروتکل در سطح مدیریت نام برد .

طبق استاندارد ISO-8498-2، دو جنبه ایمنی مدیریت در شبکه داریم: امنیت مدیریت و مدیریت در امنیت. بخش امنیت مدیریت در واقع، امنیت بسته‌های مدیریتی است که در شبکه ارسال می‌شوند. به عنوان مثال، حفظ امنیت بسته‌هایی مدیریتی که در شبکه ارسال و دریافت می‌شوند به این بخش مربوط می‌شود. پروتکل‌هایی همانند SSL ,... IPsec , TLS, در صورتی که از بسته‌های مدیریتی حمایت کنند، می‌توانند جزو این دسته باشند. (البته این پروتکل‌ها هر نوع ترافیک در شبکه را پشتیبانی می‌نمایند و فقط مختص ترافیک مدیریتی نیستند و می‌بایست هر نوع ترافیکی را محافظت نمایند.)

بخش دوم اشاره شده در استاندارد ISO-8498-2 ،ایجاد مدیریت در ایمنی شبکه و یا مدیریت امنیت می‌باشد. مدیریت امنیت پشتیبانی‌هایی است که یک پروتکل مدیریتی همانندSNMP در شبکه انجام می‌دهد تا ما به یک شبکه امن دست یابیم.

مدیریت شبکه با استفاده از مجموعه‌ای از ابزارهای کنترلی، به همراه مونیتورینگ شبکه، گزارشی از وضعیت شبکه می‌دهد و باعث می‌شود تا سیاست‌های امنیتی و کنترلی لازم اندیشیده شود. در این بخش پروتکل‌های کنترلی و مدیریتی وضعیت شبکه را کنترل می‌نمایند و تعیین می‌کنند که ترافیک و پیکربندی شبکه چگونه انجام شود.

مدیریت در شبکه، کار پیکربندی مناسب شبکه را با توجه به کاربرد هر شبکه انجام می‌دهد و مسولیت نگهداری و پشتیبانی از شبکه، محاسبه مقدار استفاده از منابع و تنظیم سیاست‌های اجرایی را بر عهده دارد. این تنظیمات افزایش ایمنی شبکه را فراهم می‌آورند.

مدیریت یک شبکه باید به صورت بلادرنگ و در کنار شبکهٔ فعال، انجام پذیرد تا در سرویس‌دهی شبکه خللی ایجاد نشود و احیانا شبکه کند نشود. ابزارهای مدیریتی شبکه، یک محیط GUI برای مدیر فراهم می‌نماید و با پیام‌های مربوطه، خطاهای شبکه را اطلاع می‌دهد. این ابزار قابلیت بررسی و تست شبکه و ترافیک آن، همچنین ثبت رویدادهای شبکه را نیز دارند. به کار بردن ابزار مدیریتی، زمان عیب‌یابی و راه‌اندازی سیستم‌ها را کاهش می‌دهد.

استانداردSNMP، یک استاندارد مونیتورینگ می‌باشد که وضعیت شبکه را بررسی نموده و دستورات لازم را ارسال می‌نماید. سه نسخه از این استاندارد به بازار آمده است. نسخه سوم استاندارد، ابعاد امنیتی احراز هویت، محرمانگی و کنترل دسترسی فیچرهای مدیریتی را پشتیبانی می‌نماید. پروتکل SNMP مربوط به لایه کاربرد بوده و می‌تواند بر روی TCP و UDP اجرا شود. البته نسخه یک تنها بر روی UDP قابل پیاده‌سازی بوده است.

این استاندارد از شماره پورت 161برای ارسال درخواست به عناصر شبکه و شماره پورت 162 برای ارسال رویدادها به ایستگاه مدیریت استفاده می‌نماید. ایستگاه مدیریتی یا(Management Agent)، کار نظارت و مدیریت را انجام

www.FarazNetwork.ir

می‌دهد و سایر عناصر موجود در شبکه تحت نظارت این ایستگاه مدیریتی فعالیت می‌نمایند. اطلاعات مدیریتی تحت ساختار(MIB(management Information Base قرار دارند. عناصر(Agent) هایی که در کار مدیریت شبکه شرکت می‌نمایند، می‌توانند Bridge ها، مسیریاب‌ها و یا هاب‌ها و یا هر عنصر دیگری باشند. مدیریت این عناصر بر عهده ایستگاه مدیریت می‌باشد که می‌تواند بیش از یک ایستگاه در نظر گرفته شود. استانداردSNMP امکان تنظیمات ایستگاه مدیریتی، بازیابی مقادیر MIB و یا اطلاعات از رویدادهایی که در هر Agent رخ می‌دهد، را با استفاده از دستورات ساده(Get, SET, Trap) به دست می‌آورد.

پروتکل SNMP ، علاوه بر مدیریت برای ایجاد امنیت شبکه، در ثبت رویدادها و به اصطلاح log management نیز کاربرد دارد. ثبت رویدادها به منظور آگاهی از رفتار شبکه انجام می‌پذیرد تا سیاست‌های مناسب کنترلی برای شبکه بر اساس نوع رویدادها،تنظیم شود و ما را به سوی داشتن شبکه امن‌تر رهنمون سازد.

بخش‌های امنیتی پروتکلSNMP

در ادامه معرفی پروتکل مدیریتی SNMP به مکانیزم‌های امنیتی آن می‌رسیم.

بخش‌های امنیتی همانند احراز هویت، محرمانگی و یکپارچگی در نسخه سومSNMP مورد توجه قرار گرفته است. در زمان انتقال پیام توسط SNMP می‌توان حالتهای دسترسیread-only, read-write, no-access را برای پیام‌ها تنظیم نمود. در نسخه 1 و 2 این پروتکل شنود بسته‌های ارسال شده قابل انجام بود زیرا رمزنگاری داده در ترافیک شبکه انجام نمی‌شد.

این پروتکل می‌تواند بر روی TCP پیاده‌سازی شود اما در اغلب موارد بر روی UDP پیاده‌سازی می‌شود که IP spoofing را در این بخش میسر می‌نماید و شنود بسته‌های داده ارسال شده در شبکه را در لایه IP قابل انجام می‌نماید.

حملات brute force (شکستن رمز با امتحان تعدادی کلید با توجه به طول کلید الگوریتم رمزنگاری) و dictionary attack از جمله مواردی هستند که تمام نسخه‌های این پروتکل نسبت به آن ضعف دارند. این ضعف به خاطر عدم پشتیبانی پروتکل ازchallenge- response handshake می‌باشد.

علاوه بر حملات بالا، این پروتکل می‌بایست در مقابل حمله dos نیز مقابله نماید. به این منظور، مقایسه پاسخ‌های دریافت شده به ازای درخواست‌های ارسال شده به شبکه در SNMP انجام می‌پذیرد. هر پاسخی که دریافت می‌شود می‌بایست به ازای درخواستی، ارسال شده به شبکه باشد؛ در غیر این صورت احتمال وجود حمله DOS وجود دارد.

در نسخه سوم این پروتکل مدل امنیتی مبتنی بر کاربر با نام ((User-based Security Model(USM) تعریف شده است. مدل USM در معماریSNMP کاربرد دارد و پروسیجرهایی تولید می‌کند تا در ایجاد سطوح امنیتی برای

www.FarazNetwork.ir

پیام‌های SNMP استفاده شوند. یکسری MIB مدیریتی برای مونیتورینگ و نظارت بر این مدل امنیتی(USM) تعریف شده است. نحوه انجام این تنظیمات در RFC 3414 تشریح شده است.

در بخش احراز هویت از الگوریتم‌های رمزنگاری HMAC-MD5-96 و HMAC-SHA-96 استفاده می‌شود و CBC-DES برای محرمانگی در پروتکلSNMP کاربرد دارد. به منظور حفظ محرمانگی، احراز هویت پیام بایستی الزامی باشد. مدل USM پروتکلSNMP امکان استفاده از این الگوریتم‌ها را در کنارSNMP مهیا نموده است.

هر کدام از الگوریتم‌ها به روشی پیاده‌سازی می‌شوند و توضیح نحوه پیاده سازی روش‌ها و الگوریتم‌های ذکرشده در بالا جزو معرفی SNMP نمی‌باشد. برای آشنایی با هر کدام از این الگوریتم‌ها می‌توانید از شبکه اینترنت استفاده نموده و شرح پیاده‌سازی آن‌ها را مطالعه نمایید. روش و مدلUSM این الگوریتم‌ها را به منظور افزایش کارایی و امنیت پروتکل SNMP در کنار هم وبه کمک واحدهایMIB پیاده سازی نموده است.

پروتکلSNMP امکان پیاده‌سازی بر روی محیطهای متعدد با کاربری در شبکه‌های وسیع و یا شبکه‌هایی با کاربردهای محدود و کوچک را دارا می‌باشد.

پروتکل SNMP برای سیستم‌های مدیریت در شبکه به منظور مونیتورینگ تجهیزات نصب شده در شبکه کاربرد دارد و شامل یک لایه کاربردی، یک پایگاه داده و بخش داده می‌باشد.
داده مدیریتی پیکربندی سیستم را توصیف می‌نماید. داده‌ها توسط کاربردهای مدیریتی تنظیم و مقداردهی می‌شوند. معماری و ساختارSNMP متشکل از مجموعه ای از ایستگاه های مدیریت شبکه و المان‌های شبکه است. المان‌های مدیریتی کاربردهای مربوط به مدیریت را اجرا می‌کنند . این المان‌ها وظیفه کنترل و مونیتورینگ تجهیزات شبکه را بر عهده دارند. SNMP ارتباط بین المان‌های مدیریتی و المان‌های شبکه را در لایه کاربردOSI برقرار می‌نماید.

هر سیستم مدیریتی با استفاده از یک بخش نرم‌افزاری(agent) اطلاعات لازم را از طریقSNMP به سیستم مدیریتی منتقل می‌نماید. همان‌طور که قبلا هم اشاره شده است،SNMP پورت161 از UDP را برایagentها و پورت 162 را برای مدیریت استفاده می‌کند. مدیریت می‌تواند درخواست‌ها را از طریق هر پورت مبدای به پورت161 یک agent بفرستد و هر agent پاسخ درخواست مدیریت را به پورت‌های مبدا می‌فرستد.

مدیریت پیام‌های هشدار و اطلاع‌رسانی را از طریق پورت162 دریافت می‌نماید، اما یک agent اجازه دارد پیام‌های هشدار و اطلاع‌رسانی را از طریق هر پورت در دسترس خود ارسال نماید.

تجهیزات شبکه که از پروتکلSNMP استفاده می‌نمایند، یک گره مدیریتی در شبکه تشکیل می‌دهند. این گره‌ها و تجهیزات مدیریتی، وظیفه جمع‌آوری و ذخیره اطلاعات مدیریتی و تبدیل آن‌ها به داده‌هایی قابل استفاده برایSNMP را بر عهده دارند.

یک agent درواقع یک ماژول نرم‌افزاری مدیریت شبکه است و در مورد داده‌های محلی گره شبکه، اطلاعات مدیریتی دارد و آن‌ها را به فرمت قابل تفسیرSNMP، ترجمه می‌نماید.

www.FarazNetwork.ir

ساختار مدیریتی توسط زیربخشی از SNMP با نام MIB و یا (Management Information Bases) تعریف می‌شود.MIB ساختار مدیریتی یک سیستم را توصیف می‌کند. هر واحدMIB با نام OID و یا (Object Identifier) نام دارد و متغیری را در بر می‌گیرد که توسطSNMP قابل خواندن و تفسیر می‌باشد. هر OID می‌تواند به لایه‌ای از OSI مربوط باشد.

پروتکلSNMP، دارای یک متعادل‌کننده بار نیز می‌باشد. این بخش(dispatcher) وظیفه مدیریت ترافیک بار را درSNMP برعهده دارد. برای بسته‌های داده‌ای که خارج می‌شوند، یکdispatcher نوع پیام و نوع پردازشی که باید روی آن انجام پذیرد، را مشخص می‌نماید. سپس پیام را به ماژول مورد نظر راهنمایی می‌نماید. Dispatcher پیام مربوطه را برای ارسال به لایه انتقال می‌سپارد .
برای پیام‌های ورودی،dispatcher پیام‌ها را از لایه انتقال دریافت می‌نماید و هر پیام را به ماژول متناظر برای پردازش می‌دهد و پیام را به کاربرد موردنظر راهنمایی می‌نماید.

www.FarazNetwork.ir