Simple Network Management Protocol

علاوه بر سطح دسترسی کاربری ، سطح مدیریت یکی از سطوح معماری شبکه است که شامل پروتکل های مختلفی می باشد و از استاندارد snmp می توان به عنوان یک پروتکل در سطح مدیریت نام برد.

یکی از معروف ترین پروتکل هایی که در مانیتورینگ استفاده می شود پروتکل snmp می باشد که مخفف کلمه Simple Network Management Protocol می باشد و معمولا در دو حالت Read Only و Read Write در سرورها فعال می شود. دستگاه های سخت افزاری شبکه اعم از سویچ ها و روترها بصورت پیشفرض بر روی خود این سرویس را فعال دارند اما این سرویس بر روی ویندوز سرور وجود ندارد و باید نصب و پیکربندی شود.

طبق استاندارد ISO-8498-2 ، دو جنبه ایمنی مدیریت در شبکه داریم:

امنیت مدیریت و مدیریت در امنیت.

بخش امنیت مدیریت در واقع، امنیت بسته های مدیریتی است که در شبکه ارسال می شوند. به عنوان مثال، حفظ امنیت بسته هایی مدیریتی که در شبکه ارسال و دریافت می شوند به این بخش مربوط می شود. پروتکل هایی همانند SSL, TLS,IPsec,... در صورتی که از بسته های مدیریتی حمایت کنند، می توانند جز این دسته باشند.

بخش دوم اشاره شده در استاندارد ISO-8498-2 ایجاد مدیریت در ایمنی شبکه و یا مدیریت امنیت می باشد.

مدیریت امنیت پشتیبانی هایی است که یک پروتکل مدیریتی همانند snmp در شبکه انجام می دهد تا ما به یک شبکه امن دست یابیم.

مدیریت شبکه با استفاده از مجموعه ای از ابزارهای کنترلی، به همراه مونیتورینگ شبکه، گزارشی از وضعیت شبکه می دهد و باعث می شود تا سیاست های امنیتی و کنترلی لازم اندیشیده شود. در این بخش پروتکل های کنترلی و مدیریتی وضعیت شبکه را کنترل می نمایند و تعیین می کنند که ترافیک و پیکربندی شبکه چگونه انجام شود.

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

MIB پایگاه اطلاعات مدیریتی در SNMP

MIB در واقع مجموعه ای از اطلاعات است که به صورت سلسله مراتبی سازماندهی شده است و از پروتکل های مدیریتی از قبیل SNMP استفاده می کند. MIBها شامل موضوعات مدیریت شده (Objects) هستند که توسط شناسه های Object Identifier مشخص می‌شوند. یك موضوع مدیریت شده که گاهی اوقات MIB نامیده می شود، در واقع یکی از مشخصه های تجهیزات مدیریت شده است.

دو نوع موضوع مدیریت شده وجود دارد:

1- Scalar Object

2- Tabular Object

موضوعات Scalar یك نمونه موضوع واحد را تعریف می‌کنند، ولی موضوعاتTabular چندین موضوع به هم پیوسته و مرتبط که به صورت گروهی در جداول MIB قرار دارند را تعریف می‌کنند. برای مثال تعداد پکتهای ورودی Apple Talk به یك اینترفیس از یك روتر با atln put معین می‌شود که یك موضوع Scalar است و یك نمونه موضوع واحد را نشان می‌دهد.

در سلسه مراتب MIB، هر موضوع برای شناسایی دارای یك شناسه Object ID است. سلسه مراتب MIB بصورت یك درخت (Nameless route) شرح داده می شود.

Object ID های بالاترین سطح، به سازمان های استاندارد سازی مختلف متعلق اند و Object ID های سطوح پایینتر به سازمانهای وابسته آن اختصاص می یابند. فروشندگان می توانند شعبات و یا شاخه هایی را تعریف کنند که شامل موضوعات مدیریت شده برای تولیدات خودشان است و MIB هایی که استاندارد نشده اند، در شاخه های آزمایشی قرار می گیرند.

برای مثال موضوعات مدیریت شده atln put می تواند بوسیله نام موضوعی ISO مشخص شود.

ایستگاه مدیریتی یا Management Agent کار نظارت و مدیریت را انجام می دهد و سایر عناصر موجود در شبکه تحت نظارت این ایستگاه مدیریتی فعالیت می نمایند. اطلاعات مدیریتی تحت ساختار management Information Base (MIB) قرار دارند.

استاندارد snmp امکان تنظیمات ایستگاه مدیریتی، بازیابی مقادیر MIB و یا اطلاعات از رویدادهایی که در هر Agent رخ می دهد، را با استفاده از دستورات ساده GET,SET,TRAP به دست می آورد.

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 می پذیرد تا سیاست های مناسب کنترلی برای شبکه بر اساس نوع رویدادها،تنظیم شود و ما را به سوی داشتن شبکه امن تر رهنمون سازد.

سه نسخه از این استاندارد به بازار آمده است. نسخه سوم استاندارد، ابعاد امنیتی احراز هویت، محرمانگی و کنترل دسترسی feature های مدیریتی را پشتیبانی می نماید.

پروتکل snmp مربوط به لایه کاربرد بوده و می تواند بر روی TCP و UDP اجرا شود.

نسخه یک تنها بر روی UDP قابل پیاده سازی بوده است.

SNMP V1

SNMP V2

SNMP V3

هر سه ورژن، دارای یک سری مشخصات مشترک هستند. البته باید افزود نسخه شماره سه بسیار ایمن تر از نسخه های دیگر است.

می توان گفت هر یک از اجزاء شبکه که از پروتکل snmp پشتیبانی کرده و می توان از آنها با استفاده از NMS ها به واسطه پروتکل snmp اطلاعات دریافت نمود، یک Managed Device خوانده می‌شود.

SNMP یک پروتکل مدیریتی توزیع شده است. لذا یک سیستم در این پروتکل می تواند بطور انحصاری به صورت یک NMS یا یک Agent یا هر دوی آنها عمل کند. NMS نیاز خواهد داشت که یک سیستم سوالی و جوابی (System query) تجهیزات را مدیریت کند و اقدام به تهیه گزارشات محلی و ذخیره اطلاعات مدیریتی کند.

SNMP فاقد هرگونه توانائی در شناسایی و تصدیق Authentication می باشد که این امر باعث آسیب پذیری در انواع سطوح امنیتی می شود که عبارتند از:

1) Masquerading (تغییر شکل رخدادها) : شامل یک اقدام غیر مجاز برای اجراء کارمندهای مدیریتی بوسیله فردی که یک عنصر مدیریتی مجاز را شناسایی کرده است.

2) Information modification (تغییر در اطلاعات) : شامل یک اقدام غیر مجاز برای تغییر یک

پیام تولید شده توسط یک عنصر مجاز است. این اقدام می تواند در مورد فرامین مربوط به مدیریت مالی و یا پیکربندی صورت گیرد.

3) Timing & message sequence modification (تغییر در توالی و زمانبندی) : این حالت وقتی رخ می دهد که یک عنصر غیر مجاز اقدام به ثبت، ضبط، کپی و یا تاخیر انداختن یک پیام تولید شده توسط یک عنصر مجاز کرده و بعدا به آن پاسخ می دهد.

4) Disclosure Results (فاش سازی نتایج) : این حالت وقتی رخ می دهد که یک عنصر غیر مجاز مقادیر ذخیره شده در موضوعات مدیریت شده را استخراج می کند و یا اینکه رخدادهای قابل توجه در حال تبادل بین Agent ها و Manager را می خواند و یاد می گیرد.