بررسی پروتکل SNMP

Simple Network Management Protocol (SNMP) :

پروتکل SNMP یک پروتکل مورد استفاده برای مدیریت شبکه می باشد.

این پروتکل برای جمع آوری اطلاعات از Configuration دستگاه های شبکه مانند سرور ها،روترها،سوئیچ و پرینتر و تمامی دستگاهی هایی که در داخل شبکه بر روی پروتکل IP فعالیت میکنند.

پروتکل SNMP شامل دو بخش میباشد :

SNMP Manager :

سیستم مدیریت شبکه که از SNMP برای نظارت و دریافت داده ها از هرتعداد از دستگاه های شبکه استفاده میکند.SNMP Manager معمولا برنامه ای است که در یک مکان مرکزی اجرا میشود.

SNMP Agent :

یک فرایند که برروی دستگاه های شبکه که تحت نظارت هستند اجرا میشود. تمامی داده ها و دیتاها توسط خود دستگاه جمع آوری شده و در یک پایگاه داده محلی ذخیره میشوند. سپس Agent میتواند به Query های SNMP با اطلاعات از دیتابیس محلی خود پاسخ دهد و میتواند Alert و Trap هارا به SNMP Manager ارسال کند.

هر سوئیچ در شبکه بصورت خودکار دیتاهای مربوط به خودش و تمامی اینترفیس هایش را جمع آوری میکند.

این دیتاها در محلی به نام Management Information Base (MIB) در Memory ذخیره شده و بصورت Real Time آپدیت میشوند.

این MIB در ساختار Hierarchical یک ساختار درختی را ایجاد میکند.بصورت ساده تمام MIB مجموعه ای از متغییر ها می باشد که در MIB های جداگانه ذخیره میشوند این این MIB ها شاخه های این درخت را تشکیل میدهند.

هر MIB براساس زبان Abstract Syntax Notation 1 (ASN.1) میباشد.هر متغییر در MIB با یک شناسه به نام object identifier(OID) وجود دارد که یک رشته ی طولانی که مسیر Root Tree تا مکان دقیق متغییر دنبال میکند.

برای دیدن هریک از اطلاعات MIB باید SNMP Manager یک SNMP Poll و یا Query را به سو.یچ ارسال کند.

این Query حاوی OID متغییری است که SNMP Manager درخواست کرده تا Agent در حال اجرا بر روی سوییچ متوجه میشود که چه اطلاعاتی برای بازگشت وجود دارد.

حال SNMP Manager میتواند با استفاده از یکسری از مکانیزم ها با SNMP Agent ارتباط برقرار کند و همچنین تمامی این ارتباط بر روی پروت UDP 161 میباشد. :

Get Request :

یک مقدار (Value) خاص MIB مورد نیاز می باشد.

Get Next Request :

مقدار بعدی از درخواست اولیه ی دریافتی مورد نیاز می باشد.

Get Bulk Request :

جدول کامل و یا لیست مقادیر در یک متغییر MIB مورد نیاز می باشد.

Set Request :

یک متغییر خاص MIB باید به یک مقدار تنظیم شود.

بعد از متوجه شدن نوع برقراری ارتباط بین SNMP Manager و SNMP Agent حال بین این دو اطلاعاتی رد و بدل میشود.

پیام های SNMP Poll و یا Request ها معمولا بصورت دوره ای توسط SNMP Manager ارسال میشوند.این مشکلاتی از قبیل سخت شدن مانتیورینگ میشود زیرا تا بازه ی بعدی متوجه مشکلات نمیشود.

با این حال SNMP Agent میتواند Alert های ناخواسته را به SNMP Managerبصورت Real-Time ارسال کند این Alert ها میتواند با مکانیزم های زیر بر روی پورت UDP 162 ارسال شوند :

SNMP Trap :

اخبار مربوط به Event های (تغییر وضعیت اینترفیس ها که UP/DOWN شدن یا خیر ، Device Failure و ...هرچیزی) بدون هیچ Ack ای که بگه این Alert ها دریافت شدن.

Informs Request :

اخبار یک Event به SNMP Manager ارسال میشود و Manager باید به Agent یک Ack مبنی بر تایید کردن اینکه اون اطلاعات دریافت شده بفرستد.

پروتکل SNMP در سه ورژن موجود می باشد :

SNMP Version 1 :

از یک متغییر ساده Get و Set Request همراه با یک SNMP Trap ساده استفاده میکند.
SNMP Manager با تطبیق یک Community text String میتواند به SNMP Agent ها دسترسی پیدا کند.

هنگامی که Manager میخواد یک متغییر MIB را در یک دستگاه بخواند و یا آنرا بنویسد یک Community String به عنوان بخشی از Request ارسال میکند.

در تئوری اینگونه بیان شده که Manager و Agent تنها به شرط یکسان بودن Community ها میتونن باهم ارتباط برقرار کنند. اما در عمل و واقعیت هردستگاه توانایی خواندن و نوشتن متغییرها به دیتایس MIB یه Agent با ارسال رشته ی Community درست و مناسب بدونه اینکه ایا اون دستگاه SNMP Manager است یا خیر که این یک حفره ی امنیتی بزرگ در SNMP ایجاد میکند.

SNMP Version 2 :

نسخه ی دوم SNMP برای رفع برخی ضعف های امنیتی و نگرانی ها بوجود اومد.

بطور مثال در SNMP V1 شمارنده ی متغییر (Variable Counters) یکم معنی کردنشون سخته :) 32 بیتی بود که در SNMP V2 به 64 بیت تغییر کرد.

علاوه بر این SNMP V2 یک Request یعنی Bulk Request را نیز عرضه میکند که در SNMP V1 وجود نداشت و با استفاده از آن میتوان متغییر های MIB را با یک Request مجزا در یک فرم بزرگ بازیابی کرد. همچنین Event های ارسال شده از یک SNMP Agent میتواند به شکل SNMP Trap و یا Inform Request اطلاع رسانی شوند.(توجه داشته باشید که Inform Request نیاز به Ack از سمته SNMP Manager دارد که تایید کند پیام دریافت شده)

نکته : در SNMP V2 هیچ یک از مشکلات امنیتی در SNMP V1 رفع نشده است. همچنین پیاده سازی های دیگری از SNMP V2 وجود داشت که با SNMP V2C ناسزگار بودند که این دو مانع از گسترش این ورژن و دلیلی برای عرضه ی ورژن جدید تر شدند.

SNMP Version 3 :

اخرین ورژن SNMP که در حال حاضر از آن استفاده میشود SNMP V3 می باشد.

در این ورژن تمامی مشکلات امنیتی که در ورژن های قبل موجود بود را رفع شده است.

ورژن SNMP 3 میتواند با استفاده از Username (نام کاربری) SNMP Manager هارا Authenticate (تایید) کند.

هنگامی که بر روی SNMP Agent ها Username کانفیگ شود میتوان آنهارا در گروه های SNMP V3 سازماندهی کرد.

همچنین دسترسی به اطلاعات هر MIB را میتوان بر اساس هر گروه کنترل کرد.میتوان تایید کرد که کدام مقدار های MIB از Tree را میتوان خواند یا نوشت.

هر گروه SNMPv3 با یک سطح امنیتی تعریف شده است که از میزان مشخصی از داده های SNMP محافظت می کند.

پکت های داده ها میتوانند Authenticate شوند برای حفظ یکپارچگی و همچنین میتوانند Encrypt شوند برای رمزگذاری داده ها و یا هردوی آنها.

ممکن است در دیدن نام آنها گیج شوید در طرح نام گذاری Auth همان Authentication و Priv همان Encryption می باشد.

حال نگاهی به این سطح های امنیتی بی اندازیم :

noAuthNoPriv :

پکت های SNMP نه Authenticate و نه Encrypt میشوند.

AuthNoPriv :

پکت های SNMP احراز هویت Authenticate میشوند اما Encrypt نمیشوند.

AuthPriv :

پکت های SNMP هم Authenticate و هم Encrypt میشوند.

به عنوان Best Practice باید از SNMP V3 برای استفاده از ویژگی های امنیتی استفاده شود.

خب دوستان این هم یک بررسی اجمالی در رابطه با پروتکل SNMP امیدوارم مفید بوده باشه.